CUK-H03254-75-0248728

75

AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

EDITED BY

WEI-LIANG CHOW
THE JOHNS HOPKINS UNIVERSITY

J. A. DIEUDONNÉ
INSTITUT DES HAUTES ETUDES SCIENTIFIQUES

A. M. GLEASON
HARVARD UNIVERSITY

PHILIP HARTMAN
THE JOHNS HOPKINS UNIVERSITY

WITH THE COÖPERATION OF

L. V. AHLFORS
A. BOREL
H. CARTAN
S. S. CHERN
C. CHEVALLEY
K. IWASAWA
K. KODAIRA
F. I. MAUTNER
J. MILNOR
A. WEIL

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

510.5

VOLUME LXXXIII

1961

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

24

AUTOSYNARTETIC SOLUTIONS OF DIFFERENTIAL EQUATIONS.*

By D. C. LEWIS.[1]

---

1. **Introduction.** We are concerned with the differential system

1.1) $$dx/dt = f(t,x),$$

where x and f are n-vectors and t is the scalar independent variable. We ıssume that f is defined and of class C' in a suitably chosen region, which we shall not need to specify in detail.

A simple and familiar example of the sort of thing we wish to study ·curs when f is periodic in t with period T. This situation may be described ·y saying that the transformation

1.2) $$s = t + T, \qquad y = x,$$

akes the equation (1.1) into the form $y' = f(s,y)$ where the accent denotes ifferentiation with respect to s. This is just the original equation in a lifferent notation. If, now, it is known that a particular solution $x(t)$ of 1.1) has the property that $x(0) = x(T)$, it is immediately obvious that $x(t)$ nust be periodic with period T; in other words, $x(t)$ must satisfy a functional quation,

1.3) $$x(t+T) = x(t),$$

least, if $x(t)$ can be defined for all values of t.

Suppose now that (1.1) is carried into itself by a more complicated ansformation than (1.2), say by the transformation,

1.4) $$s = P(t,x), \qquad y = h(t,x),$$

here P is a scalar and h a vector and both are of class C' in t and x. If, ›w, it is known that a certain solution $x(t)$ has the property that $h(0, x(0))$

---

* Received April 18, 1960.

[1] This research was partially supported by the United States Air Force through the ir Force Office of Scientific Research of the Air Research and Development Command, nder Contract Number AF 49(638)-382. Reproduction in whole or in part is per-itted for any purpose of the United States Government.

$=x(P(0,x(0)))$ it will turn out that $x(t)$ must satisfy the functiona equation,

$$x(P(t,x(t)))=h(t,x(t)), \tag{1.5}$$

at least, if $x(t)$ can be defined for all values of t.

Evidently, if $P(t,x)=t+T$ and $h(t,x)=x$, (1.4) and (1.5) reduc respectively to (1.2) and (1.3); so that the situation in which $f(t,x)$ i periodic in t is indeed a special case of what we wish to consider.

An important problem concerning the simpler situation is the perturbation of periodic solutions with respect to a parameter, a problem first considered by Poincaré. We shall show that the main features of this theory of Poincaré and his followers may be extended to cover the perturbation of a solution satisfying (1.5). Such solutions will be called autosynartetic; and we shall present theorems about the *degeneracy* of an autosynartetic solution, about the associated so-called *bifurcation equations*, about the influence of certains kinds of *first integrals* on the degeneracy and on the bifurcation equations, and about phenomena associated with the presence of certain kinds of *continuous groups* (*or semi groups*) *of transformations* which take (1.1) into itself.

For instance, when the system (1.1) is autonomous (i.e. when $f(t,x)$ $=f(x)$ is independent of t) and when therefore we may imbed the transformation (1.2) in the continuous group of transformations,

$$s=t+T+\lambda, \qquad y=x, \tag{1.6}$$

(where λ is the parameter of the group) in such a manner that (1.6) equall with (1.2) takes (1.1) into itself, the well known fact, that any non-constant periodic solution of $dx/dt=f(x)$ must be degenerate, is just a simple special case of one of our theorems on general autosynartetic solutions.

Our theories, in addition to applying to the entirely new subject of general autosynartetic solutions, may even yield a few new results about the simpler cases already studied. Thus, for instance, to the best of the author's knowledge, Theorems 8.4, 8.5, and 8.6, specialized to the periodic case, have not appeared in fully developed form in the literature, although partial results along these lines are given in [4] (cf. the References at the end of the paper). Again, in some special non-autonomous periodic case, it might be possible to imbed (1.2) in some 1-parameter transformation group,

$$s=P(t,x,\lambda), \qquad y=h(t,x,\lambda),$$

with $P(t,x,0)=t+T$ and $h(t,x,0)=x$. Our theory then says that any periodic solution of (1.1) must be degenerate, at least, if we impose one further mild condition on the periodic solution in question, which takes the place of the condition mentioned above in the autonomous case that the solution should not be a constant.

We shall also discuss necessary and sufficient conditions that (1.4) should transform (1.1) into itself, using a definition which may strike the reader as a little peculiar, since it does not require (1.4) to possess an inverse. This definition was adopted, since in the major part of the paper we never need to assume the existence of an inverse to (1.4). We shall show that infinitely many such transformations always exist, in fact, even when $P(t,x)$, as well as $f(t,x)$, is prescribed. These transformations are, however, determined by the integration of a system more complicated than (1.1) and hence cannot be expected to be of any real help in any qualitative discussion of the solutions of (1.1). Such help is to be expected only when a particular transformation is more or less obvious from the structure of the equations. Thus, for example, the equations of celestial mechanics admit both rotational and translational symmetry. It often happens, under such circumstances, that the functional equation (1.5) merely expresses the fact that $x(t)$ is in some sense a periodic solution, when suitable coordinates are employed (cf. "les trois sortes de solutions périodiques" of Poincaré [5], vol. 1, pp. 95-97). At other times it gives us periodic solutions possessing certain special properties of symmetry. An indication of how this may occur is as follows:

Suppose that, in (1.4), $P(t,x) = t + T$, while $y = h(t,x) = h_1(x)$ is independent of t and generates a finite cyclic group of transformations of order k. Then the functional equation (1.5) implies that

$$x(t + mT) = h_m(x(t)),$$

where h_m denotes the m-th iterate of h_1. Since h_k is the identity transformation, we see at once that, under present hypotheses, our functional equation expresses the fact that $x(t)$ is a certain special kind of periodic solution with period kT.

Another possibility may arise if $y = h_1(x)$ generates an infinite free group, such that, for any positive ϵ, we shall have $|h_m(x) - x| < \epsilon$ for infinitely many values of m. We then get a recurrent solution, or, if $h_m(x)$ recurs to an approximation of the identity in a suitably uniform manner, we would get an almost periodic solution.

In spite of these trivialities in the presently contemplated applications, the transformations considered in this paper can be of a much more general type, well deserving serious study for their own sake.

2. Some elementary theorems on the transformations of differential equations.

DEFINITION 2.1. *To say that* (1.4) *transforms the system* (1.1) *into the system,*

$$dy/ds = g(s,y), \tag{2.1}$$

means that to every solution $x(t)$ *of the system* (1.1) *there corresponds a solution* $y(s)$ *of* (2.1) *such that*

$$y[P(t,x(t))] = h[t,x(t)]. \tag{2.2}$$

Notice that this definition does not require (1.4) to have an inverse, although certainly one would ordinarily expect an inverse to exist in cases of principal importance.

THEOREM 2.1. *If* (1.4) *transforms* (1.1) *into* (2.1), *the functions* $h(t,x)$ *and* $P(t,x)$ *must satisfy the vector partial differential equation,*

$$\begin{aligned} &h_t(t,x) + h_x(t,x)f(t,x) \\ &\qquad = g[P(t,x),h(t,x)][P_t(t,x) + P_x(t,x)f(t,x)], \end{aligned} \tag{2.3}$$

at every point of the common domain of definition of f, P, and h.

Proof. Differentiate the identity (2.2) with respect to t and use the fact that $dy(s)/ds = g(s,y(s))$ with $s = P(t,x(t))$. We also use the facts that $dx(t)/dt = f(t,x(t))$ and consequently that

$$ds/dt = P_t(t,x(t)) + P_x(t,x(t))f(t,x(t)).$$

The result is

$$\begin{aligned} &g[P(t,x(t)),y[P(t,x(t))]] \\ &\qquad [P_t(t,x(t)) + P_x(t,x(t))f(t,x(t))] \equiv h_t(t,x(t)) + h_x(t,x(t))f(t,x(t)). \end{aligned}$$

Finally we notice that, by the existence theorem for the system (1.1), there is a solution through every point of the space where f is defined. Hence the last identity in t, based on an arbitrary solution $x(t)$ of (1.1), becomes an identity in t and x, if we eliminate y with the help of (2.2) and then replace $x(t)$ simply by x.

THEOREM 2.2. *If* $P(t,x)$ *and* $f(t,x)$ *have the property that*

$$P_t(t,x) + P_x(t,x)f(t,x) \neq 0 \tag{2.4}$$

at every point of their common domain of definition and if $h(t,x)$ *is any vector function satisfying* (2.3), *then* (1.4) *transforms* (1.1) *into* (2.1).

Proof. Let $x(t)$ be any solution of (1.1). Then by (2.4) we have

$$(d/dt)[P(t,x(t))] = P_t(t,x(t)) + P_x(t,x(t))f(t,x(t)) \neq 0.$$

Hence by the implicit function theorem, the equation

$$s = P(t,x(t)) \tag{2.5}$$

may be solved for t in terms of s. It is then easy to see from Definition 2.1 that it will be enough to prove that the vector function $y(s)$ defined as being the same as $h[t(s),x(t(s))]$ is a solution of (2.1). Remembering that $y(s(t)) = h(t,x(t))$, we see from (2.5) and (1.1) that $dy(s(t))/ds(t) = (dy/dt)/(ds/dt) = [h_t(t,x) + h_x(t,x)f(t,x)]\,[P_t(t,x) + P_x(t,x)f(t,x)]^{-1}$, where we have, of course, used x as an abbreviation for $x(t)$. We thus obtain from (2.3) the result that

$$y'(s(t)) = g[P(t,x),h(t,x)] = g[s(t),y(s(t))].$$

Changing the independent variable from t to s, we obtain the desired result.

Before passing to the next theorem, it is convenient to introduce the following further notation: Let

$$x = \xi(t,t_0,x_0) \tag{2.6}$$

be the solution of (1.1) such that

$$\xi(t_0,t_0,x_0) = x_0. \tag{2.7}$$

Let $x = \xi(t,t_0,x_0)$ together with $u = U(t,t_0,x_0,u_0)$ be the solution of the following enlarged system of order $2n$:

$$dx/dt = f(t,x), \tag{2.8a}$$

$$du/dt = G(t,x,u), \tag{2.8b}$$

where $G(t,x,h)$ is an abbreviation for $g[P(t,x),h][P_t(t,x) + P_x(t,x)f(t,x)]$, so that consequently the partial differential equation (2.3) appears in the abbreviated form

$$h_t(t,x) + h_x(t,x)f(t,x) = G[t,x,h(t,x)]. \tag{2.9}$$

The function $U(t,t_0,x_0,u_0)$ is to satisfy the condition

$$U(t,t_0,x_0,u_0) = u_0. \tag{2.10}$$

The fact, that such functions ξ and U, affording a solution of (2.8) and satisfying the initial conditions indicated by (2.7) and (2.10), actually exist, is, of course, a consequence of the known theory of ordinary differential equations.

THEOREM 2.3. *The n-vector function*

$$h(t,x)=U[t,t_0,\xi(t_0,t,x),H(\xi(t_0,t,x))] \tag{2.11}$$

satisfies the partial differential equation (2.9) (*which is the same as* (2.3)), *together with the initial condition,*

$$h(t_0,x)=H(x). \tag{2.12}$$

Here it is understood that $H(x)$ is an arbitrary n-vector function of class C'.

The proof of this theorem may be left to the reader, since a theory for the equation (2.9) in which h is a vector may be formulated exactly as if h were a scalar. Such a theory in the scalar case is given by Kamke [3], vol. 2, pp. 40-42. It may also be remarked that the verification of (2.12) is immediate with the help of (2.7) and (2.10), and that the verification of (2.9), although somewhat more complicated, may be carried out in a straightforward manner by differentiation of (2.11) and by use of well known properties of the functions ξ and U.

3. The transformation of a system of differential equations into itself.

We continue the discussion initiated in the preceding section only for the special case in which

$$g(t,x)\equiv f(t,x). \tag{3.1}$$

We also shall assume throughout the rest of the paper that the inequality (2.4) *holds.* With this understanding the following theorem is an immediate corollary of Theorems 2.1 and 2.2).

THEOREM 3.1. *A necessary and sufficient condition that* (1.4) *transform* (1.1) *into itself is that*

$$h_t(t,x)+h_x(t,x)f(t,x)=f[P(t,x),h(t,x)][P_t(t,x)+P_x(t,x)f(t,x)] \tag{3.2}$$

Similarly specializing Theorem 2.3 by (3.1), and using Theorem 3.1, we may state the obvious

THEOREM 3.2. *When* $P(t,x)$ *and* $f(t,x)$ *are given,* h *may be found in infinitely many ways in such a manner that* (1.4) *transforms* (1.1) *into itself. In fact we may assign* $h(t_0,x)$ *arbitrarily for any fixed* t_0.

DEFINITION 3.1. *If* (1.4) *transforms* (1.1) *into itself, and if* $x(t)$ *is any solution of* (1.1), *the solution* $y(t)$ *of* (1.1), (*possibly not distinct from* $x(t)$), *which is such that*

$$y[P(t,x(t))] \equiv h(t,x(t)), \tag{3.3}$$

is said to be synartetic to $x(t)$ *under the transformation* (1.4). *If* $y(t) \equiv x(t)$, *we shall term* $x(t)$ *an autosynartetic solution of* (1.1) *under* (1.4).

Notice that, under the assumptions of this definition, the existence of the $y(t)$ mentioned above is *guaranteed* by Definition 2.1.

THEOREM 3.3. *Assuming that* (1.4) *transforms* (1.1) *into itself, a necessary and sufficient condition that a solution* $y(t)$ *be synartetic to a solution* $x(t)$ *of* (1.1) *under* (1.4) *is that*

$$y[P(t_0,x(t_0))] = h(t_0,x(t_0)) \tag{3.4}$$

for any fixed t_0.

Proof. The necessity of (3.4) is obvious, since we may substitute t_0 for t in (3.3).

The sufficiency follows by an easy argument based, firstly, on the existence of a solution synartetic to a given solution, $x(t)$, as guaranteed above, and, secondly, on the uniqueness theorem for equation (1.1).

By considering the special case $y = x$, we get the following obvious corollary to Theorem 3.3, to which we must frequently refer in the later sections of this paper.

THEOREM 3.4. *Assuming that* (1.4) *transforms* (1.1) *into itself, a necessary and sufficient condition that a solution* $x(t)$ *of* (1.1) *should be autosynartetic under* (1.4) *is that*

$$x[P(t_0,x(t_0))] = h(t_0,x(t_0)) \tag{3.5}$$

for any fixed t_0.

In the next section we tacitly assume the validity of

THEOREM 3.5. *Let* $x(t,\alpha)$ *be a family of solutions of* (1.1) *which is continuous and continuously differentiable with respect to the parameter* α. *Let* $y(t,\alpha)$ *be the family of solutions of* (1.1) *synartetic under* (1.4) *to* $x(t,\alpha)$. *Then* $y(t,\alpha)$ *is also continuous and continuously differentiable.*

Proof. We may, because of (2.4), solve the equation, $s = P(t,x(t,\alpha))$

for $t = t(s, \alpha)$. Hence the solution $y(t, \alpha)$, synartetic to $x(t, \alpha)$, is given by the formula, $y(s, \alpha) = h[t(s, \alpha), x(t(s, \alpha), \alpha)]$. If h, P, and x are of class C', so is $t(s, \alpha)$, and hence eventually $y(s, \alpha)$.

4. Properties of the variational system and of its adjoint. Let us consider an arbitrary solution $x = \phi(t)$ of (1.1). The equations of variation based on this solution are

$$d\xi/dt = A(t)\xi, \tag{4.1}$$

where

$$A(t) = f_x(t, \phi(t)). \tag{4.2}$$

The equations of variation have the following familiar fundamental property: If $x = x(t, \alpha)$ is a family of solutions of (1.1) depending on a parameter α in any manner and such that $x(t, 0) \equiv \phi(t)$, then $\xi(t) = \partial x(t, 0)/\partial\alpha$ is a solution of (4.1).

Now let us suppose that (1.4) transforms (1.1) into itself. Let us denote the synartetic solution of $x(t, \alpha)$ by $y(t, \alpha)$. Then $\eta(t) = \partial y(t, 0)/\partial\alpha$ will be a solution of the system $d\eta/dt = A^*(t)\eta$ where $A^*(t) = f_x(t, \phi^*(t))$, in which $\phi^*(t) = y(t, 0)$ is of course synartetic to $x(t, 0) = \phi(t)$. Consequently, if $\phi(t)$ is *auto*-synartetic, we shall have $\phi^*(t) = \phi(t)$ and $A^*(t) \equiv A(t)$; so that η satisfies the same system (4.1) as ξ.

We now proceed to compute the relationship between ξ and η. Since $y(t, \alpha)$ is synartetic to $x(t, \alpha)$, we know that $y(s, \alpha)$ is obtained from the equations,

$$y = h(t, x(t, \alpha)) \tag{4.3}$$

$$s = P(t, x(t, \alpha)) \tag{4.4}$$

by the elimination of t. Hence

$$\delta y/\delta\alpha = \partial y/\partial\alpha + (\partial y/\partial t)(\delta t/\delta\alpha) \tag{4.5}$$

where partial derivatives obtained under the assumption that α and t are independent variables are denoted by ∂, while those obtained under the assumption that α and s are independent variables are denoted by δ. From (4.3) we obtain

$$\begin{aligned} &\partial y/\partial\alpha = h_x(t, x(t, \alpha))(\partial x/\partial\alpha) \text{ and} \\ &\partial y/\partial t = h_t(t, x(t, \alpha)) + h_x(t, x(t, \alpha))f(t, x(t, \alpha)), \end{aligned} \tag{4.6}$$

where we have simplified the last expression by using the fact that $x(t, \alpha)$

is a solution of (1.1). We further transform the last expression with the help of (3.2), thus obtaining

$$(4.7)\quad \partial y/\partial t = f[P(t,x(t,\alpha)),h(t,x(t,\alpha))]\,[P_t(t,x(t,\alpha)) + P_x(t,x(t,\alpha))f(t,x(t,\alpha))].$$

We next compute $\partial t/\partial\alpha$ from (4.4) as follows:

$$0 = \delta s/\delta\alpha = [P_t(t,x(t,\alpha)) + P_x(t,x(t,\alpha))f(t,x(t,\alpha))](\delta t/\delta\alpha) + P_x(t,x(t,\alpha))(\partial x/\partial\alpha).$$

Hence

$$\delta t/\delta\alpha = -(\partial x/\partial\alpha)P_x(t,x(t,\alpha))[P_t(t,x(t,\alpha)) + P_x(t,x(t,\alpha))f(t,x(t,\alpha))]^{-1}.$$

Using this last result together with (4.6) and (4.7) we see from (4.5) that

$$\delta y/\delta\alpha = [h_x(t,x(t,\alpha)) - f[P(t,x(t,\alpha)),\ h(t,x(t,\alpha))]{}^{\circ}P_x(t,x(t,\alpha))](\partial x/\partial\alpha).$$

Here, and throughout the remainder of the paper, $f^{\circ}P_x$ denotes the matrix of order n the element in whose i-th row and j-th column is the product of the i-th component of f by the j-th component of P_x. This is to be contrasted with the scalar product P_xf used also very frequently in this paper.

Setting $\alpha = 0$, $x(t,0) = \phi(t)$, $\delta y(s,0)/\delta\alpha = \eta(s)$ and $\partial x(t,0)/\partial\alpha = \xi(t)$, we obtain

$$(4.8)\qquad \eta(s) = B(t)\xi(t)$$

where the matrix $B(t)$ is defined by

$$(4.9)\qquad B(t) = h_x(t,\phi(t)) - f[P(t,\phi(t)),h(t,\phi(t))]{}^{\circ}P_x(t,\phi(t)),$$

or, since $\phi(t)$ is autosynartetic, by

$$(4.9\text{ alt.})\qquad B(t) = h_x(t,\phi(t)) - f[P(t,\phi(t)),\phi(P(t,\phi(t)))]{}^{\circ}P_x(t,\phi(t)),$$

and where the s of (4.8) is related to the t by means of (4.4) with the $\alpha = 0$, in other words by

$$(4.10)\qquad s = P(t,\phi(t)) = p(t).$$

We interpret and summarize the main results of this discussion in the following:

THEOREM 4.1. *The variational system of* (1.1) *based on an autosynartetic solution* $\phi(t)$ *of* (1.1) *under* (1.4) *is transformed into itself by means of the transformation*

$$(4.11)\qquad s = p(t),\qquad \eta = B(t)\xi,$$

where the scalar function $p(t)$ *and the matrix function* $B(t)$ *are given respectively by* (4.10) *and by* (4.9).

Proof. According to Definition 2.1, we need only to show that to every *arbitrary* solution $\xi(t)$ of (4.1) there corresponds a solution $\eta(t)$ of (4.1) such that $\eta(p(t)) = B(t)\xi(t)$, or, in other words, such that (4.8) holds with s given by (4.10). Our previous discussion therefore yields a complete proof, as soon as it is established that an *arbitrary* solution $\xi(t)$ can be represented in the form $\partial x(t,0)/\partial\alpha$ used above. This is an elementary detail which we leave to the reader.

An almost immediate corollary of Theorem 4.1 is

THEOREM 4.2. *Between the matrices* $A(t)$, $B(t)$, *and the scalar* $p(t)$ *there is the following relationship:*

$$dB(t)/dt + B(t)A(t) - A(p(t))B(t)(dp(t)/dt) \equiv 0. \tag{4.12}$$

Proof. Since (4.11) transforms (4.1) into itself we may apply the partial differential equation (3.2), with appropriate changes of notation, to the present linear situation. In this way we obtain the result that $(dB(t)/dt)\xi + B(t)A(t)\xi = A(p(t))B(t)\xi(dp(t)/dt)$. But, since this is an identity in the vector ξ, we obtain (4.12) at once.

It is also possible to verify (4.12) directly from the definitions of $A(t)$, $B(t)$, and $p(t)$ and from the fact that h satisfies (3.2). But the calculation is rather tedious. From such an alternative proof of Theorem 4.2, we also have an alternative proof for Theorem 4.1, which follows from Theorem 4.2 with the help of Theorem 3.1.

At this stage, it is convenient to introduce the function $q(t)$ which is the inverse of $p(t)$, so that

$$p(q(t)) = q(p(t)) = t. \tag{4.13}$$

This is legitimate, since by (4.10) and (2.4),

$$\dot{p}(t) = P_t(t, \phi(t)) + P_x(t, \phi(t))f(t, \phi(t))$$

is never zero. We also introduce the matrix $C(t)$ defined by

$$C(t) = B(q(t))'. \tag{4.14}$$

The accent is used here and in the remainder of the paper to denote the transpose of a matrix.

THEOREM 4.3. *The linear system*

$$(4.15)\qquad d\xi/dt = -A(t)'\xi \quad \text{or} \quad d\xi/dt = -\xi A(t),$$

which is the so-called adjoint to the system (4.1), *is transformed into itself by means of the transformation,*

$$(4.16)\qquad s = q(t), \qquad \eta = C(t)\xi.$$

Proof. From Theorem 3.1, as in the proof of the previous theorem, we find that a necessary and sufficient condition that (4.5) be transformed into itself by (4.16) is the validity of the identity

$$(4.17)\qquad dC(t)/dt - C(t)A(t)' + A(q(t))'C(t)(dq(t)/dt) \equiv 0.$$

If we replace t by $p(t)$ and then multiply by dp/dt we get the equivalent identity,

$$\begin{aligned}&[dC(p(t))/dp](dp(t)/dt) - C(p(t))A(p(t))'(dp(t)/dt)\\ &\qquad + A[q(p(t))]'C(p(t))(dq(p(t))/dp)(dp(t)/dt) \equiv 0.\end{aligned}$$

This, with the help of (4.13) and (4.14), is seen to be equivalent to

$$dB(t)'/dt - B(t)'A(p(t))'(dp(t)/dt) + A(t)'B(t)' \equiv 0.$$

But this last identity is merely the transpose of (4.12). Thus we have shown that (4.17) is equivalent to the already established identity (4.12).

THEOREM 4.4. *In order that a solution $\xi(t)$ of the variational equations* (4.1) *be autosynartetic under the transformation* (4.11) *it is necessary and sufficient that it satisfy the "boundary conditions,"*

$$(4.18)\qquad \xi(T) = B\xi(0),$$

where

$$(4.19)\qquad T = p(0) \quad \text{and} \quad B = B(0).$$

Proof. This is a special case of Theorem 3.4 applied to the linear system under (4.11) instead of to the general system (1.1) under (1.4). And, in making this application, we take $t_0 = 0$.

THEOREM 4.5. *In order that a solution $\xi(t)$ of the adjoint system* (4.15) *be autosynartetic under the transformation* (4.16) *it is necessary and sufficient that it satisfy the boundary conditions*

$$(4.20)\qquad \xi(T)B = \xi(0)$$

where T and B are given by (4.19).

Proof. Again appealing to Theorem 3.4, we find that a necessary and sufficient condition that $\xi(t)$ be autosynartetic under (4.16) is that $\xi[q(T)] = C(T)\xi(T)$. In obtaining this result we take the t_0 of Theorem 3.4 to be T. From (4.13) and (4.14), we find that $q(T) = 0$ and that $C(T) = B'$, whence it appears that (4.20) is an equivalent condition.

Whenever we refer to autosynartetic solutions of the variational system or its adjoint, we always mean autosynarteticity under (4.11), in the case of the variational system, and under (4.16) in the case of the adjoint system. Thus, according to Theorems 4.4 and 4.5, autosynartetic solutions of the variational equations are those which satisfy the boundary conditions (4.18) and autosynartetic solutions of the adjoint equations are those which satisfy the boundary conditions (4.20). With this understanding we have

THEOREM 4.6. *The maximum number of solutions in any set of linearly independent autosynartetic solutions of the variational equations* (4.1) *is equal to the maximum number of solutions in any set of linearly independent autosynartetic solutions of the adjoint system* (4.15).

Proof. Let the $n \times n$ matrix $X(t)$ satisfy $dX/dt = A(t)X$ and $\det X(0) \neq 0$. Hence $\det X(t) \neq 0$. Corresponding to any arbitrary solution $\xi(t)$ of the variational equations, there exists an n-vector c such that $\xi(t) = X(t)c$, and, by Theorem 4.4, this is autosynartetic under (4.11) if and only if $X(T)c = BX(0)c$, which is equivalent to $X(T)^{-1}[X(T) - BX(0)]c = 0$. *Hence the number of linearly independent autosynartetic solutions of the variational equations is equal to the number of linearly independent relationships between the columns of the matrix* $X(T)^{-1}[x(T) - BX(0)]$.

Now, if we set $Y(t)' = X(t)^{-1}$, it is well known (and indeed easy to see by differentiation of $Y(t)'X(t) = I$) that $dY/dt = -A(t)'Y$ and det $Y(t) \neq 0$. Hence, corresponding to any arbitrary solution $\xi_1(t)$ of the adjoint system, there exists an n-vector c_1 such that $\xi_1(t) = Y(t)c_1$, and, by Theorem 4.5, this is autosynartetic under (4.16) if and only if $[Y(T)c_1]B = Y(0)c_1$ or $c_1Y(T)'B = c_1Y(0)'$. In terms of $X(t)$ this condition appears (after some simple manipulations) in the equivalent form $c_1X(T)^{-1}[X(T) - BX(0)] = 0$. *Hence the number of linearly independent autosyartetic solutions of the adjoint system is equal to the number of linearly independent relationships between the rows of the matrix* $X(T)^{-1}[X(T) - BX(0)]$.

The theorem follows at once from the above two italicized sentences.

5. Synartetic first integrals and so-called degeneracy. First integrals are defined in the usual way; namely a scalar function $J(t,x)$ is called a first integral of (1.1), if its value is independent of t whenever x is replaced by any solution $x(t)$ of (1.1). It is both obvious and well known that a necessary and sufficient condition that J be a first integral is that

$$J_t(t,x)+J_x(t,x)f(t,x)\equiv 0, \tag{5.1}$$

at least, if J is of class C'.

If (1.1) is transformed into itsef by (1.4), then with every solution $x(t)$ of (1.1) there is associated a synartetic solution $y(t)$. Hence, if $J(t,x)$ is a first integral of (1.1), we see that $J(s,y(s))$ must be independent of s. Hence, setting $s=P(t,x(t))$ and remembering that then $y(s)=h(t,x(t))$ by definition of a synartetic solution, we see that $J[P(t,x(t)),h(t,x(t))]$ must be independent of t no matter with what solution $x(t)$ we may be dealing. In other words, we have established

THEOREM 5.1. *If* $J(t,x)$ *is a first integral of* (1.1) *and if* (1.1) *is transformed into itself by* (1.4), *then* $J[P(t,x),h(t,x)]$ *is also a first integral of* (1.1).

DEFINITION 5.1. *Under the assumptions of Theorem* 5.1, *the first integral* $J[P(t,x),h(t,x)]$ *is said to be synartetic to the first integral* $J(t,x)$; *and, if it happens that*

$$J[P(t,x),h(t,x)]\equiv J(t,x), \tag{5.2}$$

we shall say that the first integral $J(t,x)$ *is autosynartetic under* (1.4).

THEOREM 5.2. *Let* $\phi(t)$ *be an autosynartetic solution of* (1.1) *under* (1.4). *Let* $J(t,x)$ *be an autosynartetic first integral of* (1.1) *also under* (1.4). *Then* $\xi(t)=J_x(t,\phi(t))$ *is an autosynartetic solution of the adjoint system* (4.15) *of the equations of variation* (4.1).

Proof. Differentiating (5.2) with respect to x and then setting $x=\phi(t)$ and $p(t)=P(t,\phi(t))$, we find that

$$J_t[p(t),h(t,\phi(t))]P_x(t,\phi(t))+J_x[p(t),h(t,\phi(t))]h_x(t,\phi(t))\equiv J_x(t,\phi(t)).$$

But according to (5.1) we know that

$$J_t[p(t),h(t,\phi(t))]=-J_x[p(t),h(t,\phi(t))]f[p(t),h(t,\phi(t))].$$

Hence, eliminating $J_t[p(t),h(t,\phi(t))]$ and remembering that $h(t,\phi(t))=\phi(p(t))$, since ϕ is autosynartetic, we find that

$$J_x[p(t),\phi(p(t))]\,[h_x(t,\phi(t))-f[p(t),h(t,\phi(t))]^{\circ}P_x(t,\phi(t))]=J_x(t,\phi(t)).$$

Thus, remembering that $p(t) = P(t, \phi(t))$ and $\xi(t) = J_x(t, \phi(t))$, we find from (4.9) that $\xi(p(t))B(t) = \xi(t)$. Setting $t = 0$, we find from (4.19) that $\xi(t)$ satisfies the boundary condition (4.20). It remains to show that $\xi(t)$ satisfies the adjoint system (4.15). Since this may be done as in the periodic special case, we leave this part of the proof to the reader. See Lewis [4], p. 542, lines 23-37, where, however, the notation as well as the context must be modified to fit present circumstances.

DEFINITION 5.2. *The degeneracy of an autosynartetic solution* $\phi(t)$ *of the system* (1.1) *is equal to the maximum number of solutions of the variational equations* (4.1) *in any set of linearly independent autosynartetic solutions of these equations or, what by Theorem* 4.6 *is the same thing, the maximum number of solutions of the adjoint equations* (4.15) *in any set of linearly independent autosynartetic solutions of the adjoint equations.*

If there are no autosynartetic solutions of (4.1) other than the trivial solution $\xi \equiv 0$, the degeneracy is of course 0 by the definition, and we then sometimes say that $\phi(t)$ is *non-degenerate.*

THEOREM 5.3. *If the system* (1.1) *admits* k *"independent" autosynartetic first integrals, then the degeneracy of any autosynartetic solution* $\phi(t)$ *of* (1.1) *is at least* k.

Here the hypothesis that the k first integrals should be independent is interpreted as meaning that the rank of the jacobian matrix of the k integrals with respect to the components of x should be k when $x = \phi(t)$. This insures the existence of k linearly independent autosynartetic solutions of the adjoint system as indicated in Theorem 5.2, so that no further proof is needed for Theorem 5.3.

THEOREM 5.4. *If* (1.1) *admits a* k*-parameter family of autosynartetic solutions, the degeneracy of any one of the solutions imbedded in the family is at least* k.

Proof. Suppose the k-parameter family of autosynartetic solutions of (1.1) is represented by $x = x(t, c)$, where c is a k-vector and $x(t, 0) = \phi(t)$. Then the k columns of the nxk matrix $x_c(t, 0)$ are obviously solutions of the variational equations (4.1) based on $\phi(t)$. Moreover, since $x(t, c)$ for each fixed c is given as autosynartetic under (1.4), we have from Theorem 3.4

$$x[P(0, x(0, c)), c] = h(0, x(0, c)).$$

Differentiating with respect to c and then setting $c=0$ and also using the fact that $x(t,c)$ is a solution of (1.1) we obtain

$$f[P(0,\phi(0)),\phi[P(0,\phi(0))]]^{\circ}P_x(0,\phi(0))x_c(0,0)+x_c[P(0,\phi(0)),0]$$
$$=h_x(0,\phi(0))x_c(0,0),$$

which, because of (4.9 alt.), (4.10), and (4.19), can be written

$$x_c(T,0)=Bx_c(0,0).$$

Hence $x_c(t,0)$ satisfies the boundary conditions specified in Theorem 4.4. The fact that $x(t,c)$ is actually a k-parameter family means also that the rank of the matrix $x_c(t,c)$ is k. Thus, the k columns of $x_c(t,0)$ yield k linearly independent autosynartetic solutions of the variational equations, so that, by Definition 5.2, the degeneracy of $\phi(t)$ must be at least k.

THEOREM 5.5. *Assume that the set of all transformations which transform* (1.1) *into itself contains a continuous family F of transformations of class C' satisfying the following three conditions:*

P1. *Every transformation of F commutes with* (1.4).

P2. *F contains the identity transformation.*

P3. *There is a solution $\phi(t)$ which is autosynartetic under* (1.4) *but which is not autosynartetic under any transformation of F close to the identity* (*except under the identity itself*).

Then $\phi(t)$ has degeneracy $\geqq 1$.

Proof. A transformation S which transforms (1.1) into itself according to Definition 2.1 provides a mapping of the set of all solutions of (1.1) into itself. Namely S maps an arbitrary solution x of (1.1) onto the solution y which is synartetic to x under S. We express this mapping by writing $Sx=y$. Let S^* denote the transformation (1.4) and let S_λ denote a transformation of F, where λ represents a set of values for the parameters of F. We may suppose by P2 that S_0 is the identity transformation.

By P3, we have $S^*\phi=\phi$. Hence $S_\lambda S^*\phi=S_\lambda\phi$. Whence, from P1, we obtain $S^*S_\lambda\phi=S_\lambda\phi$. Hence $S_\lambda\phi$ is autosynartetic under S^*. Hence by P2, $\phi=S_0\phi$ is imbedded in a continuous family of solutions $\{S_\lambda\phi\}$ each of which is autosynartetic under S^*, i.e. under (1.4). Because of P3, $S_\lambda\phi\neq\phi$ for λ close to 0, except for $\lambda=0$. Hence the number of essential parameters in our family of autosynartetic solutions is surely greater than zero. Hence by Theorem 5.4 the degeneracy of ϕ is greater than zero, as we wished to prove.

In the above theorem the family F does not necessarily form a group. In fact, our Definition 2.1 does not require the transformations which "transform (1.1) into itself" to have inverses: In fact, if $\{x\}$ is the set of all solutions x of (1.1) and if S is a transformation transforming (1.1) into itself, the set $\{Sx\}$ of all synartetic solutions under S can be a proper subset of $\{x\}$.

If, however, the transformation S^* (i.e. (1.4)) is an element of a full differentiable continuous group G of transformations taking (1.1) into itself, we know from the theory of Lie that G possesses a one-parameter continuous abelian subgroup F also containing S^*. Hence the conditions P1 and P2 are automatically satisfied in this case. This is the situation, mentioned in Section 1, which occurs in the classical theory of periodic solutions of autonomous systems.

6. Perturbation of autosynartetic solutions. We now suppose that the system (1.1) contains a parameter μ and that the same may also be true of the transformation (1.4). We therefore write

$$dx/dt = f(t, x, \mu) \tag{6.1}$$

instead of (1.1), and

$$s = P(t, x, \mu), \qquad y = h(t, x, \mu) \tag{6.2}$$

instead of (1.4). We suppose that the dependence of f, P, and h on μ is of class C' and that (6.1) is transformed into itself by the transformation (6.2) for each value of μ, such that $|\mu| < \beta$.

THEOREM 6.1. *Let $\phi(t)$ be a nondegenerate autosynartetic solution of* (6.1) *under the transformation* (6.2) *when $\mu = 0$. Then there exists a positive number $\beta^* \leqq \beta$, such that* (6.1), *for $|\mu| < \beta^*$, admits an autosynartetic solution $x(t, \mu)$ under the transformation* (6.2). *Moreover the dependence of $x(t, \mu)$ on μ is of class C' and $x(t, \mu) \to \phi(t)$ as $\mu \to 0$, and $x(t, \mu)$ is the only autosynartetic solution of* (6.1) *in a suitably chosen neighborhood of $\phi(t)$.*

Proof. According to Theorem 3.4 (with $t_0 = 0$), a necessary and sufficient condition that a solution $x(t, \mu)$ be autosynartetic under (6.2) is that

$$x[P(0, x_0, \mu), \mu] - h(0, x_0, \mu) = 0, \tag{6.3}$$

where $x_0 = x_0(\mu) = x(0, \mu)$. Suppose $\psi(t, x_0, \mu)$ is the solution of (6.1) such that $\psi(0, x_0, \mu_0) = x_0$. Then (6.3) may be rewritten

$$(6.4) \qquad \psi[P(0, x_0, \mu), x_0, \mu] - h[0, x_0, \mu] = 0,$$

which we wish to solve for x_0 as a function of μ for $|\mu|$ sufficiently small, already knowing, of course, that (6.4) is satisfied by $x_0 = \phi(0)$ when $\mu = 0$. A straightforward calculation of the Jacobian J of the left member of (6.4) with respect to x_0 at $\mu = 0$, $x_0 = \phi(0)$, leads, with the help of (4.19), (4.10) and (4.9 alt.) to the result, $J = X(T) - BX(0)$, where $T = P(0, \phi(0), 0) = p(0)$ and where $X(t) = \psi_{x_0}(t, \phi(0), 0)$ is a matrix solution of the variational equations (4.1), set up using $f(t, x, 0)$ of (6.1) in place of the $f(t, x)$ of (1.1). If $\det J$ were zero, there would exist a vector $c \neq 0$ such that $[X(T) - BX(0)]c = 0$, and then according to Theorem 4.4, $\xi(t) = X(t)c$ would be a non-trivial autosynartetic solution of the variational equations, contrary to the hypothesis that $\phi(t)$ is non-degenrate. Thus $\det J \neq 0$, and applying the implicit function theorem, we write $x(t, \mu) = \psi(t, x_0(\mu), \mu)$. This $x(t, \mu)$ is easily seen to have the properties stated in the theorem.

Most of the details in this proof are left to the reader because of the similarity to the well known periodic special case.

7. Lemmas on non-homogeneous linear systems. In order to give a satisfactory analysis of the perturbation of autosynartetic solutions which are not non-degenerate, we cite the following lemma which is a slight variation of Lemma 1 in [4].

LEMMA 7.1. *Consider the linear differential system*

$$(7.1) \qquad d\xi/dt = A(t)\xi + f(t),$$

where ξ and f are n-vectors and A is an $n \times n$ matrix. A and f are known continuous functions of t, defined on the closed interval $\langle 0, T \rangle$ between 0 and T (T may be either positive or negative, but not zero). Let $X(t)$ be any $n \times n$ matrix, such that $dX/dt = A(t)X$ and $\det X(0) \neq 0$ (and hence also $\det X(t) \neq 0$ for any t on $\langle 0, T \rangle$). Let $n - k$ denote the rank of the $n \times n$ matrix $BX(0) - X(T)$, where B is a constant $n \times n$ matrix. Thus k is the number of linearly independent solutions of the homogeneous system corresponding to (7.1) satisfying the "autosynartetic" boundary condition, $B\xi(0) = \xi(T)$.

Then there exist (independently of f) a $k \times n$ matrix function $\Xi(s)$ and an $n \times n$ matrix $G(t, s)$, both continuous, except that $G(t, s)$ possesses a finite jump at $t = s$, having the following properties:

(I) *The system* (7.1) *possesses a solution satisfying the boundary condition* $B\xi(0)=\xi(T)$, *if and only if*

$$\int_0^T \Xi(s)f(s)\,ds=0. \tag{7.2}$$

(II) *If* (7.2) *is satisfied, the vector function,*

$$\xi(t)=\int_0^T G(t,s)f(s)\,ds$$

is a solution of (7.1) *and is, moreover, the only solution satisfying the boundary condition* $B\xi(0)=\xi(T)$ *which is orthogonal to every solution of the corresponding homogeneous system taken with the same boundary condition.*

(III) *Whether* (7.2) *is satisfied or not,* $\xi(t)$, *defined by* (7.3), *satisfies the boundary condition* $B\xi(0)=\xi(T)$.

(IV) *The rows of* $\Xi(s)$ *are orthogonal to the rows of* $G(t,s)$. *That is,*

$$\int_0^T G(t,s)\Xi(s)'\,ds=0. \tag{7.4}$$

(V) *The* $k\times k$ *matrix,*

$$C=\int_0^T \Xi(s)\Xi(s)'\,ds, \tag{7.5}$$

is nonsingular.

This Lemma may be regarded as well known. See for example [6], where however, the Lemma does not appear in exactly the desired form. In Lewis [4], pp. 537-540, will be found a complete proof[2] in the special case $B=I$. Only trivial modifications are needed in this proof to establish the lemma in its present form. Although we shall thus omit the proof of Lemma 7.1, we must record for future use certain supplementary facts.

Since $(n-k)$ is the rank of $BX(0)-X(T)$, there is a $k\times n$ matrix $\mathfrak{A}$ and an $n\times k$ matrix $\mathfrak{B}$, both of rank k, such that

$$\mathfrak{A}[BX(0)-X(T)]=0, \qquad [BX(0)-X(T)]\mathfrak{B}=0. \tag{7.6}$$

In terms of $\mathfrak{A}$, the $k\times n$ matrix function $\Xi(s)$ of the Lemma may be taken as

---

[2] There is one formula in this proof which is in error. Namely the last formula on p. 539 should be $R(t)=\int_0^T G(t,s)\Xi(s)'C^{-1}ds$. This error fortunately does not effect the validity of the rest of the proof.

$$\Xi(s) = \mathfrak{A}X(T)X(s)^{-1}. \tag{7.7}$$

Cf. Lewis [4], p. 537, formula (2.9). The k rows of $\Xi(t)$ are also seen to afford a full set of linearly independent autosynartetic solutions of the adjoint system (4.15). This is established with the help of (7.6), Theorems 4.5, 4.6, and the well known fact that the rows of $X(t)^{-1}$ satisfy the adjoint system.

Finally

$$\det\left[\int_0^T \mathfrak{B}'X(t)'X(t)\mathfrak{B}\,dt\right] \neq 0. \tag{7.8}$$

Cf. Lewis [4], p. 538, formula (2.15) and the accompanying discussion, in which it is shown that the matrix in question is positive definite.

LEMMA 7.2. *Under the same hypotheses as in the previous lemma and using the same notation, the following $(n+k)\times(n+k)$ matrix has a non-zero determinant:*

$$\mathfrak{M} = \left\| \begin{matrix} [BX(0) - X(T)] & \int_0^T X(T)X(s)^{-1}\Xi(s)'ds \\ \int_0^T \mathfrak{B}'X(t)'X(t)\,dt & \mathfrak{K} \end{matrix} \right\|$$

where the block in the upper left hand corner (viz. $BX(0) - X(T)$) is an $n\times n$ matrix, while the block in the lower right hand corner (viz. $\mathfrak{K}$) is an arbitrary $k\times k$ matrix.

Proof. Suppose $\det\mathfrak{M} = 0$. Then there would exist a linear relationship between the columns of $\mathfrak{M}$ with coefficients which would not all be zero. In other words, *there would exist an n-vector β and a k-vector α, whose components are not all zero such that*

$$[BX(0) - X(T)]\beta + \left[\int_0^T X(T)X(s)^{-1}\Xi(s)'ds\right]\alpha = 0, \tag{7.9}$$

$$\left[\int_0^T \mathfrak{B}'X(t)'X(t)\,dt\right]\beta - \mathfrak{K}\alpha = 0. \tag{7.10}$$

Consider now the n-vector function

$$\xi(t) = X(t)\beta - \int_0^t X(t)X(s)^{-1}\Xi(s)'\alpha\,ds. \tag{7.11}$$

This $\xi(t)$ clearly satisfies the equation (7.1) in the special case that $f(t) = -\Xi(t)'\alpha$. Moreover (7.9) expresses the fact that $\xi(t)$ satisfies the boundary condition, $B\xi(0)=\xi(T)$. Hence Lemma 7.1 assures us, by means of (7.2), that

$$\int_0^T \Xi(s)\Xi(s)'\alpha\, ds = C\alpha = 0.$$

Referring now to (V) of Lemma 7.1, we conclude that $\alpha=0$. Thus $\xi(t)=X(t)\beta$, whereas (7.10) expresses the fact that $\xi(t)$, which we already know satisfies the boundary condition, is also orthogonal to every solution, satisfying the same boundary condition, of the homogeneous equation $d\xi(t)/dt=A(t)\xi(t)$. In particular $\xi(t)$ must be orthogonal to itself. Hence it must vanish identically, i.e. $X(t)\beta=0$, and since $X(t)$ is non-singular, we conclude that $\beta=0$. With both α and β necessarily reducing to zero, we have reached a contradiction of the above italicized statement resulting from the assumption that $\det\mathfrak{M}=0$. This is all that is needed to establish the lemma.

8. The bifurcation equations in the degenerate cases. Suppose that $\phi(t)$ is an autosynartetic solution of (6.1) under the transformation (6.2) when $\mu=0$. We consider the variational equation (4.1) with $A(t)=f_x(t,\phi(t),0)$. We suppose that $\phi(t)$ has degeneracy k, which means that (4.1) has just k linearly independent solutions satisfying the boundary conditions (4.18). In referring in this way to the material of Section 4, we mean that the $f(t,x)$, $h(t,x)$ and $P(t,x)$ of Section 4 are to be identified with the $f(t,x,0)$, $h(t,x,0)$, and $P(t,x,0)$ respectively of this Section or Section 6.

We define the $n\times n$ matrix $X(t)$ by the two conditions

$$dX(t)/dt=A(t)X(t), \qquad X(0)=I, \tag{8.1}$$

and then introduce the matrices $\mathfrak{A}$, $\mathfrak{B}$, $\Xi(t)$ as in Section 7.

THEOREM 8.1. *It is possible to define a unique n-vector function $x(t,c,\mu)$ and a k-vector function $\alpha(c,\mu)$ of class C' for sufficiently small c and $|\mu|$, where c is a k-vector, in such a manner that the following four conditions are fulfilled:*

$$x_t(t,c,\mu)=f[t,x(t,c,\mu),\mu]-\Xi(t)'\alpha(c,\mu) \tag{8.2}$$

$$x[P(0,x(0,c,\mu),\mu),c,\mu]=h[0,x(0,c,\mu),\mu] \tag{8.3}$$

$$\int_0^T \mathfrak{B}'X(t)'[x(t,c,\mu)-\phi(t)-X(t)\mathfrak{B}c]\,dt=0 \tag{8.4}$$

(8.5) $$x(t,0,0)=\phi(t).$$

Proof. We introduce the n-vector function $\psi(t,x_0,\alpha,\mu)$ in such a manner that

(8.6) $$x=\psi(t,x_0,\alpha,\mu)$$

is the solution of the differential system,

(8.7) $$\dot{x}=f(t,x,\mu)-\Xi(t)'\alpha$$

which reduces to x_0, when $t=0$. That is,

(8.8) $$\psi(0,x_0,\alpha,\mu)=x_0.$$

Other more or less obvious properties of ψ are the following:

(8.9) $$\psi(t,\phi(0),0,0)=\phi(t).$$

(8.10) $$\psi_{x_0}(t,\phi(0),0,0)=X(t).$$

(8.11) $$\psi_\alpha(t,\phi(0),0,0)=\sigma(t)=-\int_0^t X(t)X(s)^{-1}\Xi(s)'ds,$$

where σ is an $n\times k$ matrix which vanishes when $t=0$ and satisfies the system $d\sigma/dt=A(t)\sigma-\Xi(t)'$. To give some indication of how these properties are derived, we remark that (8.9) follows from the uniqueness theorem for (8.7) and the definition of $\phi(t)$. We derive (8.10) when we substitute $\psi(t,x_0,\alpha,\mu)$ for x in (8.7), differentiate with respect to x_0, set $x_0=\phi(0)$, $\mu=0$, $\alpha=0$, and use the definition of $A(t)=f_x(t,\phi(t),0)$ and (8.1). We get (8.11) in a similar manner by differentiting with respect to α. The expression for $\sigma(t)$, of course, comes from the Lagrange result for "variation of parameters."

We next try to find x_0 and α as functions of c and μ in such a manner that, when the functions are inserted in (8.6), $\psi(t,x_0(c,\mu),\alpha(c,\mu),\mu)$ reduces to the required $x(t,c,\mu)$ satisfying conditions (8.2), (8.3), (8.4), and (8.5). No matter how $x_0(c,\mu)$ and $\alpha(c,\mu)$ are chosen (8.2) is automatically satisfied because ψ was defined to be a solution of (8.7); and, if furthermore we require that

(8.12) $$x_0(0,0)=\phi(0),$$

(8.13) $$\alpha(0,0)=0,$$

we see that (8.5) is also satisfied because of (8.9). The other two conditions (8.3) and (8.4) lead to the following vector equations for the determination of x_0 and α as functions of c and μ.

$$(8.14) \qquad -\psi[P(0,\psi(0,x_0,\alpha,\mu),\mu),x_0,\alpha,\mu]+h[0,\psi(0,x_0,\alpha,\mu),\mu]=0.$$

$$(8.15) \qquad \int_0^T \mathfrak{B}'X(t)'[\psi(t,x_0,\alpha,\mu)-\phi(t)-X(t)\mathfrak{B}c]\,dt=0.$$

We note first of all that, consistently with (8.12) and (8.13), the last two equations (viz. (8.14) and (8.15)) are satisfied when $x_0=\phi(0)$, $\alpha=0$, $c=0$, and $\mu=0$. This is because (8.9) and the fact that $\phi[P(0,\phi(0),0)] = h[0,\phi(0),0]$, since ϕ is given as an autosynartetic solution of $\dot{x}=f(t,x,0)$ under the transformation $s=P(t,x,0)$, $y=h(t,x,0)$.

Hence, if we can show that the jacobian of the system furnished by (8.14) and (8.15) with respect to the components of x_0 and α does not vanish when $x_0=\phi(0)$, $\alpha=0$, $c=0$, and $\mu=0$, these equations, (8.14) and (8.15), by the implicit function theorem, effectively give the required functions $x_0(c,\mu)$ and $\alpha(c,\mu)$ for sufficiently small values of c and μ. Hence the proof of Theorem 8.1 will be complete as soon as we show that this jacobian is not 0.

Differentiating the left member of (8.14) with respect to x_0 and then setting $x_0=\phi(0)$, $\alpha=0$, $\mu=0$, gives with the help of (8.9) and (8.10) the following:

$$h_x[0,\phi(0),0]X(0)-\psi_t[P(0,\phi(0),0),\phi(0),0,0]^\circ P_x(0,\phi(0),0)-X(P(0,\phi(0),0)),$$

which, from the facts that $X(0)=I$, that $P(0,\phi(0),0)=T$ and that ψ satisfies (8.7) and (8.9), can be written in the form,

$$[h_x[0,\phi(0),0]$$
$$\qquad -f[P(0,\phi(0),0),\phi(P(0,\phi(0),0)),0]^\circ P_x(0,\phi(0),0)]X(0)-X(T).$$

Hence, from (4.9 alt.) and (4.19), we find that the jacobian matrix of (8.14) with respect to the components of x_0 at the point in question is the $n\times n$ matrix $BX(0)-X(T)$, which is just the block of elements in the upper left hand corner of the matrix $\mathfrak{M}$ of Lemma 7.2.

Differentiating the left member of (8.14) with respect to α, using (8.11) and evaluating at $x_0=\phi(0)$, $\alpha=0$, $\mu=0$, yields

$$\int_0^T X(T)X(s)^{-1}\Xi(s)'ds,$$

which is the block of elements in the upper right hand corner of $\mathfrak{M}$.

Differentiating the left member of (8.15) with respect to x_0 yields in a similar manner the $k \times n$ matrix,

$$\int_0^T \mathfrak{B}' X(t)' X(t)\, dt,$$

which is the block of elements in the lower left corner of $\mathfrak{M}$.

Differentiating the left member of (8.15) with respect to x_0 yields in a certain $k \times k$ matrix $\mathfrak{K}$, whose properties need no further investigation and which furnishes the block of elements in the lower right corner of $\mathfrak{M}$.

In other words, the jacobian we are interested in turns out to be $\det \mathfrak{M}$, which we know from Lemma 7.2 is not zero. This establishes Theorem 8.1, except for a few details which we leave to the reader.

THEOREM 8.2. *If the k-vector c and the scalar μ satisfy the k-vector equation,*

$$\alpha(c, \mu) = 0, \tag{8.16}$$

then the n-vector function $x(t, c, \mu)$ is an autosynartetic solution of (6.1) *under the transformation* (6.2). *Here it is understood that $\alpha(c, \mu)$ and $x(t, c, \mu)$ are as introduced in Theorem* 8.1.

Proof. Because of (8.2) and (8.16), $x(t, c, \mu)$ is a solution of (6.1). Because of (8.3) and Theorem 3.4 (with $t_0 = 0$, etc.), $x(t, c, \mu)$ is also autosynartetic.

THEOREM 8.3. *If $\bar{x}(t)$ is an autosynartetic solution of* (6.1) *under* (6.2) *and if $|\mu|$ and $|x(t) - \phi(t)|$ are sufficiently small, there exists a k-vector c such that* (8.16) *is satisfied and such that $\bar{x}(t) \equiv x(t, c, \mu)$.*

Proof. Using the function $\psi(t, x_0, \alpha, \mu)$ introduced at the beginning of the proof of Theorem 8.1 (cf. (8.6)), we see from the uniqueness theorem for differential equations that

$$\bar{x}(t) = \psi(t, \bar{x}(0), 0, \mu). \tag{8.17}$$

Since $\bar{x}(t)$ is given as autosynartetic under (6.2), Theorem 3.4 shows that $\bar{x}[P(0, \bar{x}(0), \mu)] = h(0, \bar{x}(0), \mu)$, or, using (8.17), we get

$$\psi[P(0, \bar{x}(0), \mu), \bar{x}(0), 0, \mu] = h(0, \bar{x}(0), \mu). \tag{8.18}$$

Since $\bar{x}(0) = \psi(0, \bar{x}(0), 0, \mu)$, we see from (8.18) that (8.14) is satisfied by $x_0 = \bar{x}(0)$ and $\alpha = 0$.

We define the k-vector c by means of the system of linear equations

$$(8.19) \qquad \int_0^T \mathfrak{B}'X(t)'[\psi(t,\bar{x}(0),0,\mu)-\phi(t)-X(t)\mathfrak{B}c]\,dt=0.$$

The determinant of this system in the components of c is seen by (7.8) to be different from zero. Hence (8.19) gives a valid definition of c; and moreover $|c|$ will be small if $|\mu|$ and $|\bar{x}(0)-\phi(0)|$ are sufficiently small. With this value of c we see, by comparing (8.19) with (8.15), that the latter equation is satisfied by $x_0=\bar{x}(0)$ and $\alpha=0$.

But the complete implicit function theorem contains a statement to the effect that there are no solutions near the given solution except those furnished by the implicitly defined functions. Applying this statement to the system (8.14)-(8.15), and using the notation $x_0(c,\mu)$, as well as $\alpha(c,\mu)$, introduced in the proof of Theorem 8.1, we find that $\bar{x}(0)=x_0(c,\mu)$ and $0=\alpha(c,\mu)$. Hence by (8.17) we have

$$x(t,c,\mu)=\psi[t,x_0(c,\mu),\alpha(c,\mu),\mu]=\psi[t,\bar{x}(0),0,\mu]=\bar{x}(t),$$

as we wished to prove.

DEFINITION 8.1. *The k-vector function $\alpha(c,\mu)$ being introduced as in Theorem* 8.1, *the k-vector equation* (8.16) (*or the system of k scalar equations* (8.16)) *will be called the bifurcation equation* (*or equations*) *for the autosynartetic solution $\phi(t)$ of degeneracy k.*

Theorems 8.2 and 8.3 may be summarized by the statement that the problem of the perturbation of an autosynartetic solution of degeneracy k can always be reduced to the problem of solving a system of k "bifurcation" equations instead of the generally larger system of n equations like (6.4). An example of the advantage of using bifurcation equations is indicated in the following

THEOREM 8.4. *Suppose that the system* (6.1) *admits l independent autosynartetic first integrals of class C' in t, x, and μ. Suppose also that for $\mu=0$, $\phi(t)$ is a given autosynartetic solution of* (6.1) *of degeneracy $k\geqq l$; and suppose that the k-vector function $\alpha(c,\mu)$ is set up as in Theorem* 8.1. *Then there exists an $l\times k$ matrix function $Q(c,\mu)$ of rank l* (*when $|c|$ and $|\mu|$ are sufficiently small*), *such that*

$$(8.20) \qquad Q(c,\mu)\alpha(c,\mu)\equiv 0.$$

Proof. Let the l autosynartetic first integrals be represented as the components of the l-vector $\Lambda(t,x,\mu)$. From Theorem 5.2, we know that the rows of the $l\times n$ matrix $\Lambda_x(t,x,\mu)$ evaluated for $x=\phi(t)$ and $\mu=0$ are autosynartetic solutions of the adjoint to the variational equations. Since also the $k \times n$ matrix $\Xi(t)$ of (7.7) is such that its k rows afford a full set of linearly independent autosynartetic solutions of the adjoint system it is clear that the rows of $\Lambda_x(t, \phi(t), 0)$ are linear combinations of the rows of $\Xi(t)$. In other words there exists a constant $l \times k$ matrix D such that

$$\Lambda_x(t, \phi(t), 0) = D\Xi(t). \tag{8.21}$$

Moreover, since the l first integrals are independent $\Lambda_x(t, \phi(t), 0)$, and hence D, must be of rank l. If now we define the $l \times n$ matrix

$$\zeta(t, c, \mu) = \Lambda_x(t, x(t, c, \mu), \mu) - D\Xi(t), \tag{8.22}$$

where $x(t, c, \mu)$ has the meaning explained in Theorem 8.1, we see from the continuity of $x(t, c, \mu)$ and of $\Lambda_x(t, x, \mu)$ and from (8.21) that $\zeta(t, c, \mu) \to 0$ uniformly on any finite t-interval as $|c|$ and $|\mu| \to 0$.

Since $\Lambda(t, x, \mu)$ is a vector first integral, we have

$$\Lambda_t(t, x, \mu) + \Lambda_x(t, x, \mu) f(t, x, \mu) \equiv 0.$$

In this identity, we replace x by the vector $x(t, c, \mu)$ of Theorem 8.1 and integrate from 0 to

$$T(c, \mu) = P(0, x(0, c, \mu), \mu). \tag{8.23}$$

We thus obtain

$$\int_0^{T(c,\mu)} \Lambda_x(t, x(t, c, \mu), \mu) f(t, x(t, c, \mu), \mu)\, dt + \int_0^{T(c,\mu)} \Lambda_t(t, x(t, c, \mu), \mu)\, dt \equiv 0. \tag{8.24}$$

Since Λ is autosynartetic, we have (by Definition 5.1)

$$\Lambda(t, x, \mu) \equiv \Lambda(P(t, x, \mu), h(t, x, \mu), \mu). \tag{8.25}$$

Setting $t = 0$, $x = x(0, c, \mu)$, and remembering that $h(0, x(0, c, \mu), \mu) = x(T(c, \mu), c, \mu)$ by Theorem 8.1 and (8.23), we find from (8.25) that $\Lambda[T(c, \mu), x(T(c, \mu), c, \mu), \mu] - \Lambda(0, x(0, c, \mu), \mu) \equiv 0$. Hence

$$\int_0^{T(c,\mu)} (d/dt)[\Lambda[t, x(t, c, \mu), \mu]]\, dt \equiv 0.$$

Hence

$$(8.26)\qquad \int_0^{T(c,\mu)} \Lambda_x[t, x(t,c,\mu),\mu]x_t(t,c,\mu)\,dt + \int_0^{T(c,\mu)} \Lambda_t[t, x(t,c,\mu),\mu]\,dt \equiv 0.$$

Substracting (8.26) from (8.24) yields

$$\int_0^{T(c,\mu)} \Lambda_x[t, x(t,c,\mu),\mu]\,[f(t, x(t,c,\mu),\mu) - x_t(t,c,\mu)]\,dt \equiv 0.$$

But, from (8.2), this last identity may be written

$$\int_0^{T(c,\mu)} \Lambda_x[t, x(t,c,\mu),\mu]\,\Xi(t)'\alpha(c,\mu)\,dt \equiv 0.$$

We therefore obtain (8.20), if we let

$$Q(c,\mu) = \int_0^{T(c,\mu)} \Lambda_x(t, x(t,c,\mu),\mu)\,\Xi(t)'\,dt.$$

Evidently from (8.22)

$$Q(c,\mu) = D\int_0^T \Xi(t)\Xi(t)'\,dt + D\int_T^{T(c,\mu)} \Xi(t)\Xi(t)'\,dt + \int_0^{T(c,\mu)} \zeta(t,c,\mu)\Xi(t)'\,dt.$$

Now $T(c,\mu) \to T(0,0) = T$ as $c \to 0$ and $\mu \to 0$ and $\zeta(t,c,\mu) \to 0$ uniformly. We also know that $\int_0^T \Xi(t)\Xi(t)'\,dt$ is a non-singular $k \times k$ matrix (cf. Lemma 7.1 (V)). It therefore follows that $Q(c,\mu)$ must, like D, have the rank l for $|c|$ and $|\mu|$ sufficiently small.

A simple corollary of Theorem 8.4 is the following

THEOREM 8.5. *If there are l independent autosynartetic first integrals, the perturbation of any autosynartetic solution of degeneracy k (necessarily $\geqq l$ by Theorem 5.3) may be effected by the solution of $k - l$ of the bifurcation equations, the other l bifurcation equations being then automatically satisfied. In particular, if $k = l$, the bifurcation equations are all identically satisfied.*

Proof. Since $Q(c,\mu)$ is of rank l, we may solve (8.20) for l of the components of α, say, $\alpha_1, \cdots, \alpha_l$ in terms of the other components $\alpha_{l+1}, \cdots, \alpha_k$ so that we have equations of the form

$$\alpha_i(c,\mu) = \sum_{j=l+1}^{k} q_{ij}(c,\mu)\alpha_j(c,\mu), \qquad i = 1, \cdots, l.$$

Hence, if $\alpha_j(c,\mu) = 0$ for $j = l+1, \cdots, k$, we also have $\alpha_i(c,\mu) = 0$ for $i = 1, \cdots, l$.

THEOREM 8.6. *Suppose that the system* $dx/dt = f(t,x,0)$ *admits* l *independent autosynartetic first integrals of class* C' *in* t *and* x *(even though the system* $dx/dt = f(t,x,\mu)$ *for* $\mu \neq 0$ *may not). Suppose also that* $\phi(t)$ *is a given autosynartetic solution of* (6.1) *under* (6.2) *when* $\mu = 0$ *and that the k-vector function* $\alpha(c,\mu)$ *is set up as in Theorem* 8.1. *Then there exists an* $l \times k$ *matrix function* $Q(c)$ *of rank* l, *when* $|c|$ *is sufficiently small, such that*

$$Q(c)\alpha(c,0) \equiv 0. \tag{8.27}$$

Proof. Consider the modified system $dx/dt = f^*(t,x,\mu)$ where $f^*(t,x,\mu) \equiv f(t,x,0)$ is a constant with respect to variation in μ. Then the given l autosynartetic first integrals of $\dot{x} = f(t,x,0)$, which are also independent of μ, are autosynartetic first integrals of $dx/dt = f^*(t,x,\mu)$ under the modified transformation $s = P^*(t,x,\mu) \equiv P(t,x,0)$, $y = h^*(t,x,\mu) \equiv h(t,x,0)$. Hence Theorem 8.4 applies to the modified system under the modified transformation and we get an $l \times k$ matrix, $Q^*(c,\mu)$, of rank l for $|\mu|$ and $|c|$ sufficiently small, such that

$$Q^*(c,\mu)\alpha^*(c,\mu) \equiv 0, \tag{8.28}$$

where $\alpha^*(c,\mu)$ is to the modified system as $\alpha(c,\mu)$ is to the original system. The fact that $\alpha^*(c,\mu) = \alpha(c,0)$ follows from the following two facts: (I) The equations for the determination of $\alpha^*(c,\mu)$ and $x^*_0(c,\mu)$, namely equations (8.14) and (8.15) set up for the modified system, are seen to be completely independent of μ, so that $\alpha^*(c,\mu) = \alpha^*(c,0)$. (II) These same equations are identical with the original equations (8.14) and (8.15) when $\mu = 0$, so that $\alpha^*(c,0) = \alpha(c,0)$. Thus, from 8.28), we find that $Q^*(c,\mu)\alpha(c,0) \equiv 0$, from which we get (8.27) by choosing $Q(c) = Q^*(c,0)$.

We next turn to the consideration of properties of the bifurcation equations not dependent on the existence of autosynartetic first integrals. The *general* situation is exhaustively treated in the next two theorems.

THEOREM 8.7. *The left hand member of the bifurcation equation* (8.16) *always possesses the following two properties:*

$$\alpha(0,0) = 0 \tag{8.29}$$

$$\alpha_c(0,0) = 0. \tag{8.30}$$

Proof. From (8.5) and (8.2) we have

$$d\phi(t)/dt = f[t,\phi(t),0] - \Xi(t)'\alpha(0,0).$$

But $\phi(t)$ was given at the outset as a solution of (6.1) when $\mu = 0$. Hence

$$d\phi(t)/dt = f[t,\phi(t),0].$$

Therefore $\Xi(t)'\alpha(0,0) = 0$. From (7.7) we know that the rank of Ξ is k. Hence $\alpha(0,0) = 0$.

Incidentally, this simple proof of (8.29) or (8.13) as a necessary consequence of (8.2) and (8.5) is one of the details left to the reader at the end of the proof of Theorem 8.1. It is a step in the proof of the *uniqueness* part of Theorem 8.1.

We next establish (8.30) as follows: With the help of (8.8) we write equation (8.14) in the form,

$$\psi[P(0,x_0,\mu),x_0,\alpha,\mu] - h(0,x_0,\mu) = 0.$$

This equation is satisfied by $x_0 = x_0(c,\mu)$ and $\alpha = \alpha(c,\mu)$. Hence, upon setting $\mu = 0$, we obtain

$$\psi[P(0,x_0(c,0),0),x_0(c,0),\alpha(c,0),0] - h(0,x_0(c,0),0) = 0.$$

Differentiating with respect to c, freely using the various properties of ψ indicated in formulas (8.6) to (8.11), and also remembering the definition of $B(0)$ given by (4.9 alt.), we find, on setting $c = 0$ and $x_0(0,0) = \phi(0)$, that

$$-B(0)(\partial x_0/\partial c) + X[P(0,\phi(0),0)](\partial x_0/\partial c) \\ + \sigma[P(0,\phi(0),0)](\partial\alpha(0,0)/\partial c) = 0.$$

Since $B(0) = B$, $X(0) = I$, and $P(0,\phi(0),0) = T$, we therefore have

$$[X(T) - BX(0)](\partial x_0/\partial c) + \sigma(T)(\partial\alpha(0,0)/\partial c) = 0.$$

Hence, from (7.6), $\mathfrak{A}\sigma(T)(\partial\alpha(0,0)/\partial c) = 0$, while from (8.11), (7.7), and (V) of Lemma 7.1, we see that

$$\mathfrak{A}\sigma(T) = -\mathfrak{A}\int_0^T X(T)X(s)^{-1}\Xi(s)'ds = -\int_0^T \Xi(s)\Xi(s)'ds$$

is a non-singular matrix, so that (8.30) follows immediately.

THEOREM 8.8. *The bifurcation equations in general have no distinctive properties other than those specified in Theorem* 8.7. *More precisely:*

Let $\beta(c,\mu)$ *be an arbitrary* k*-vector function of the* k*-vector* c *and the scalar* μ. *Let* $\beta(c,\mu)$ *be of class* C', *and let it vanish together with its first partial derivatives with respect to the components of* c *when* $c = 0$ *and* $\mu = 0$. *Let* n *be any integer* $\geqq k$ *and suppose* T *is any positive number. Then there exists a system* (6.1) *of order* n *such that* $f(t+T,x,\mu) \equiv f(t,x,\mu)$, *which possesses, for* $\mu = 0$, *a periodic solution of period* T *and degeneracy* k, *and whose bifurcation equations are* $\beta(c,\mu) = 0$.

Proof. We proceed to set up such a system. For this purpose, the first k components of the n-vector x will be thought of as a k-vector x', while the last $(n-k)$ components of x will be called the $(n-k)$-vector x''. Let $A''(t)$ be any $(n-k)\times(n-k)$ matrix of continuous periodic functions of t of period, T, such that the linear system $dx''/dt = A''(t)x''$ has no non-trivial periodic solution. $A''(t)$ could be a constant matrix, if desired. Then it is claimed that the system

$$(8.31) \qquad dx'/dt = \beta(x',\mu), \qquad dx''/dt = A''(t)x'',$$

admits, for $\mu = 0$, the periodic solution $x' = 0$, $x'' = 0$, and that the bifurcation equations (8.16) for the perturbation of this solution are such that

$$(8.32) \qquad \alpha(c,\mu) \equiv \beta(c,\mu),$$

where, of course, it is understood that $\alpha(c,\mu)$ is to constructed so as to satisfy the conditions of Theorem 8.1. Since $\beta_{x'}(0,0) = 0$, the variational equations take the form

$$d\xi'/dt = 0, \qquad d\xi''/dt = A''(t)\xi''.$$

The $n\times n$ matrix solution $X(t)$ of this system such that $X(0) = I$ is seen to have the form

$$X(t)=\begin{pmatrix} I' & 0 \\ 0 & X''(t) \end{pmatrix},$$

where I' is the $k\times k$ identity matrix while $X''(t)$ is an $(n-k)\times(n-k)$ matrix, no linear combination of whose columns is periodic, while $X''(0)=I''$, the $(n-k)\times(n-k)$ identity matrix. In formula (7.6) the matrices B, $\mathfrak{A}$, and $\mathfrak{B}$ should now evidently be interpreted as follows:

$$B=I, \qquad \mathfrak{A}=(I',0), \qquad \mathfrak{B}=\begin{pmatrix} I' \\ 0 \end{pmatrix}.$$

From (7.7) we then find that $\Xi(s)=(I',0)$ so that $\Xi(t)'\alpha=\begin{pmatrix} I'\alpha \\ 0 \end{pmatrix}=\begin{pmatrix} \alpha \\ 0 \end{pmatrix}$. Hence (8.2) becomes

$$\text{(I)} \qquad \begin{aligned} x'_t(t,c,\mu)&=\beta(x'(t,c,\mu),\mu)-\alpha \\ x''_t(t,c,\mu)&=A''(t)x''(t,c,\mu). \end{aligned}$$

The condition (8.3) reduces, of course, to

$$\text{(II)} \qquad x'(T,c,\mu)=x'(0,c,\mu), \qquad x''(T,c,\mu)=x''(0,c,\mu).$$

From the fact that $\phi(t)\equiv 0$ in the present example, a routine calculation shows that (8.4) reduces to

$$\text{(III)} \qquad \int_0^T (x'(t,c,\mu)-c)\,dt=0,$$

while (8.5) is simply

$$\text{(IV)} \qquad x(t,,0,0)=0.$$

According to Theorem 8.1, these conditions determine $x(t,c,\mu)$ and $\alpha(c,\mu)$ *uniquely*. But we see by inspection that all conditions are satisfied, if we take $x'(t,c,\mu)=c$, $x''(t,c,\mu)=0$, and $\alpha=\alpha(c,\mu)=\beta(c,\mu)$. This completes the proof of (8.32) and, therefore, of the theorem.

We close this section with a brief consideration of the case when (6.1) is transferred into itself by a family of transformations,

$$\text{(8.33)} \qquad s=P(t,x,\mu,\lambda), \qquad y=h(t,x,\mu,\lambda),$$

where the parameter λ is a scalar, or, more generally an m-vector. The base solution $\phi(t)$ for $\mu=0$ is supposed to be autosynartetic under (8.33) for $\mu=0$ and $\lambda=0$. We proceed exactly as in the earlier case when the transformation did not depend on λ; only now our bifurcation equation (as well as the function $x(t, c, \mu)$ of Theorem 8.1) will depend on λ. We therefore write our bifurcation equation in the form,

$$\alpha(c, \mu, \lambda) = 0. \tag{8.34}$$

Evidently the presence of the new variable λ increases the probability of our being able to solve the bifurcation equations. Thus (8.34) may have no solution for which $\mu \neq 0$ and $\lambda = 0$, but it might very well have some for which $\mu \neq 0$ and $\lambda \neq 0$. In the latter case, we are led to an autosynartetic solution of (6.1) under (8.33) for values of $\lambda \neq 0$.

The most familiar case in which this situation arises is in the perturbation of a non-constant periodic solution of an autonomous system. Some remarks about how this case fits into our general theory have already appeared in Sections 1 and 5.

9. **Miscellaneous comments.** The reader may notice that the author has abandoned the method of integral equations used in his previous papers, especially [3]. The reason for this is primarily that the interval of integration, which would be between 0 and $P(0, x(0, \mu), \mu)$ is, in general, dependent on the unknown solution $x(t, \mu)$ as well as upon the parameter μ. A secondary reason is that the autosynartetic boundary conditions for the variational equations are not the same (in general) for different autosynartetic solutions. In the special case, when $P(t, x, \mu)$ is independent of both x and μ and $h(t, x)$ is linear and homogeneous in x, as is the case in the study of the perturbation of nonautonomous periodic solutions, these objections are no longer valid. In such cases the integral equation method is entirely feasible and, indeed, would afford the best available method of estimating the μ-interval over which perturbation is possible.

Likewise the reader will observe that only a part of Lemma 7.1 is essential for the purposes of the present paper. In particular no use is made of the "generalized Green's matrix," $G(t, s)$. Nevertheless, for the sake of completeness and in view of the indispensability of this $G(t, s)$ for the integral equation method in the fairly general case mentioned above when it is feasible and useful to employ this technique, it seemed desirable to take the opportunity of presenting Lemma 7.1 in its complete form.

Our theory of the bifurcation equation, when specialized to the periodic case, is seen to parallel very closely a theory outlined by Friedrichs [1]. Friedrichs, however, would seem to replace our condition (8.4) by a condition of the form,

$$\omega x(0, c, \mu) = c, \tag{9.1}$$

where ω is a constant $k \times n$-matrix, while c is a k-vector, as before. The present author felt that (8.4) was a more "natural" condition, perhaps because of his previous exposure to the work of Ernst Hölder [2]. It is probably possible to include both conditions, namely (8.4) and (9.1), under a more general condition, if we tamper somewhat with our Lemma 7.1, using a more generalized notion of orthogonality, which would involve the use of weight factors and Stieltjes integration. Such a generalization would probably be a mere tour de force devoid of substantially new results.

THE JOHNS HOPKINS UNIVERSITY AND RIAS.

REFERENCES.

[1] K. O. Freidrichs, "Fundamentals of Poincaré's theory," *Proceedings of the Symposium on Non-linear Circuit Analysis,* Polytechnic Institute of Brooklyn, 1953, pp. 56-67.

[2] Ernst Hölder, "Mathematische Untersuchungen zur Himmelsmechanik," *Mathematische Zeitschrift,* vol. 31 (1930), pp. 197-257.

[3] E. Kamke, *Differentialgleichungen, Lösungsmethoden, und Lösungen,* Akademische Verlagsgesellschaft, Leipzig, 1956.

[4] D. C. Lewis, "On the role of first integrals in the perturbation of periodic solutions," *Annals of Mathematics,* vol. 63 (1956), pp. 535-548.

[5] Henri Poincaré, *Les méthodes nouvelles de la mécanique céleste,* Gauthier-Villars, Paris, 1892.

[6] W. T. Reid, "Generalized Green's matrices for compatible systems of differential equations," *American Journal of Mathematics,* vol. 53 (1931), pp. 443-459.

CALCULATION OF CLASS NUMBERS BY DECOMPOSITION INTO THREE INTEGRAL SQUARES IN THE FIELDS OF $2^{\frac{1}{2}}$ AND $3^{\frac{1}{2}}$.*[1]

By HARVEY COHN.[2]

---

12. Introduction. The results presented here are a continuation of earlier results on modular functions of two complex variables of the author [16] relating to the field of $2^{\frac{1}{2}}$ and $3^{\frac{1}{2}}$. Their significance is that these results broaden the range of those modular functions which illustrate elegant properties too refined to be concluded wholly from such vast theoretical structures as that of Siegel [15]. The results have, in addition, a useful relationship to class-number calculations, which we proceed to summarize.

Consider the real quadratic field $R(D^{\frac{1}{2}})$ with discriminant $D > 0$, and, within the field, consider a totally positive integer $\mu (\gg 0)$ which might be specialized to be rational. (When $D = 1$, the field will be taken as rational.) We assume μ to be square-free for simplicity. We let $H(D^{\frac{1}{2}}, (-\mu)^{\frac{1}{2}})$ denote the class number of $R(D^{\frac{1}{2}}, (-\mu)^{\frac{1}{2}})$ and we let $A_3(\nu)$ denote the number (possibly zero) of decompositions of type

$$\nu = \xi_1^2 + \xi_2^2 + \xi_3^2, \tag{12.1}$$

where ξ_i are integers in $R(D^{\frac{1}{2}})$ and every permutation or change of sign in the triple (ξ_1, ξ_2, ξ_3) is tallied as an additional decomposition.

The class-number relationships which concern us, have essentially the form

$$\begin{cases} A_3(\mu\gamma^2) = G \cdot H(D^{\frac{1}{2}}, (-\mu)^{\frac{1}{2}}) \\ \mu \text{ square-free and totally positive } (\gg 0), \end{cases} \tag{12.2}$$

where $D = 1, 5, 8$, and 12. The factor γ^2 is needed in (12.2) because when $D = 8$ or 12, ν must belong to $\mathfrak{O}_2$ the ring of integers ν of $R(D^{\frac{1}{2}})$ of form $a + bD^{\frac{1}{2}}$. Thus even if $\mu \notin \mathfrak{O}_2$, we can conclude $\mu\gamma^2 \in \mathfrak{O}_2$ when we set

---

* Received May 6, 1960.

[1] Work supported by Research Grant G-7412 of the National Science Foundation. Presented to the American Mathematical Society, January 27, 1960.

[2] The numbering of sections and bibliographical items is consecutive with the earlier paper [16]. With the exception of some general theorems of § 7 (et al.) this paper has self-contained proofs, but perpetuates the earlier notation.

$$(12.3)\qquad \begin{cases} \gamma = 1 & \text{for } D = 1, 5, \\ \gamma = 1 & \text{for } D = 8, 12 \text{ and } \mu \in \mathfrak{O}_2, \\ \gamma = 2^{\frac{1}{2}} & \text{for } D = 8 \text{ and } \mu \notin \mathfrak{O}_2, \\ \gamma = 1 + 3^{\frac{1}{2}} & \text{for } D = 12 \text{ and } \mu \notin \mathfrak{O}_2. \end{cases}$$

The values of G are given in the accompanying table. These values depend on the manner in which the ideal (2) factors in $R(D^{\frac{1}{2}}, (-\mu)^{\frac{1}{2}})$ into distinct prime ideal factors $\mathfrak{p}$, $\mathfrak{q}$. A list of cases based on easily recognized residue classes is given in the adjoining column:

D	G	Factors of (2)	Residue classes of μ
1	0	$\mathfrak{p}\mathfrak{q}$	7 (mod 8)
(Gauss).	24	$\mathfrak{p}$	3 "
	12	$\mathfrak{p}^2$	misc. "
5	96	$\mathfrak{p}\mathfrak{q}$	$7, 3, (13 \pm 5^{\frac{1}{2}})/2, (9 \pm 3 \cdot 5^{\frac{1}{2}})/2$ (mod 8)
(Maass)	120	$\mathfrak{p}$	$5 \pm 2 \cdot 5^{\frac{1}{2}}, (5 \pm 5^{\frac{1}{2}})/2, (9 \pm 5 \cdot 5^{\frac{1}{2}})/2$ "
	12	$\mathfrak{p}^2$	misc.
8	48	$\mathfrak{p}^2\mathfrak{q}^2$	$7, 5 + 2 \cdot 2^{\frac{1}{2}}$ (mod $4 \cdot 2^{\frac{1}{2}}$)
	96	$\mathfrak{p}^2$	$3, 1 + 2 \cdot 2^{\frac{1}{2}}$ "
	24	$\mathfrak{p}^4$	misc. "
12	24*	$\mathfrak{p}^2\mathfrak{q}^2$	7, 5 (mod $4(1 + 3^{\frac{1}{2}})$)
	48*	$\mathfrak{p}^2$	3, 1 "
	12*	$\mathfrak{p}^4$	misc. "

(* See further explanation below.)

Here, for simplicity, we have further restricted μ to the case where the fields $R(D^{\frac{1}{2}})$ and $R(D^{\frac{1}{2}}, (-\mu)^{\frac{1}{2}})$ have precisely the same units. The exceptions are as follows (ignoring factors of μ which are squares for $R(D^{\frac{1}{2}})$):

$$(12.4)\qquad \begin{cases} \mu = 1, 3 & \text{for } D = 1, 5, 8, 12, \\ \mu = (5 + 5^{\frac{1}{2}})/2 & \text{for } D = 5, \\ \mu = 2 + 3^{\frac{1}{2}} & \text{for } D = 12. \end{cases}$$

In the first three cases, a complex root of unity is introduced into $R(D^{\frac{1}{2}}, (-\mu)^{\frac{1}{2}})$ and in the last case a new fundamental unit $(-2 - 3^{\frac{1}{2}})^{\frac{1}{2}}$ is introduced that was not present in $R(D^{\frac{1}{2}})$. An independent calculation reveals that in the cases (12.4) the class number $H(D^{\frac{1}{2}}, (-\mu)^{\frac{1}{2}})$ is unity, when $D = 1, 5, 8$. (A formula of type (20.16) below, reconciles these exceptions.)

The basic formula (12.2) fails, however, when $D = 12$ (see * in the table), and the formula (12.2) is an "approximation" valid only to the extent described in the next section. Considering $D = 8$, we know *for any integers a, b with $a > |b| 8^{\frac{1}{2}}$, we can represent*

$$(12.5) \qquad a + 2b2^{\frac{1}{2}} = (x_1 + y_1 2^{\frac{1}{2}})^2 + (x_2 + y_2 2^{\frac{1}{2}})^2 + (x_3 + y_3 2^{\frac{1}{2}})^2$$

in terms of integers x_i, y_i. Thus a theorem for three squares supersedes the one for four squares in the earlier work [16]. The preponderance of numerical data [3] makes it impossible, however, to reject the hypothesis that three squares suffice for $D = 12$.

13. Remarks on method. There are three different methods for establishing a formula of type (12.2). The first method is the method of Gauss which is based on a direct connection between the enumeration of quadratic forms and representations like (12.1). This method as been applied with success only to the rational case, $D = 1$.

The other two methods involve the use of some kind of theta series $\Theta(\tau)$. The function $\Theta^3(\tau)$ is, by some means or other, expanded into a "singular series" $\Psi(\tau)$ to yield identity (12.3) through a comparison of coefficients, as did Jacobi in his classic proof for $\Theta^4(\tau)$ in the rational field.

There are differences, however, in general methods for establishing $\Theta^3 = \Psi$, the basic identity. The "direct" method was applied (to the Θ^8 case) by Kronecker [4, p. 109], (see Mordell's version [23]), but in the rational case only, $(D = 1)$.

We shall see that, in the quadratic case, Θ^3 and Ψ satisfy a system of linear functional equations (like that in § 16 below), which happens to make for a one-parameter family of solutions. This method could have been used for $D = 5$ by Maass; we shall use it for $D = 8$ (as done earlier [16] for Θ^4). Indeed, the identities in § 24 are almost identical to those that would emerge for $D = 5$, so, in effect, an alternate proof of Maass' result [12] is provided by this paper.

The less direct but deeper method is due to Siegel [15] and is based on the fact that the form $\xi_1^2 + \xi_2^2 + \xi_3^2$ in $R(D^{\frac{1}{2}})$ is the only equivalence class in its genus. The method was carried out by Maass for $D = 1$ [21], and $D = 5$ [12]; (the discovery of the role of the Θ-function and class number in modular functions is due to Hecke [17]).

It should be remarked that, however straightforward it may be, the *calculation* of the singular series §§ 14-21 is a formidable matter, although the "proof proper" consists of §§ 22-24, where it is proved that $\Theta^3 - \Psi = 0$ for $D = 8$.

We shall see that when $D = 12$, $\Theta^3 - \Psi$ is a cusp-form not identically zero as evidenced by the failure of equation (12.2), or more specifically by the failure at its source (20.16), below. The case $D = 12$, however, as the case of four squares, appears to be within the scope of some kind of *exact* formula for (say) $A_3(\mu\gamma^2)$. For example, preliminary calculations show formula (12.2) to be correct when $D = 12$, if μ is a square-free rational integer > 1 and relatively prime to 6.

A continuing study for three and four square representations when $D = 12$ is being undertaken with exact formulas as a goal.

Calculation of Singular Series.

14. Notation. We continue the earlier notation with Greek letters denoting algebraic integers, Roman letters denoting rational integers (except for special function-theoretic symbols), and the generalized Norm N and Trace S applicable to conjugates in $R(D^{\frac{1}{2}})$ and our two so-called "conjugate" continuous variables τ and τ', (each complex).

We consider the two fields with given discriminant and generator:

$$\begin{cases} D = 8, & \eta = 2^{\frac{1}{2}}, \\ D = 12, & \eta = 1 + 3^{\frac{1}{2}}. \end{cases} \tag{14.1}$$

They share the properties of being Euclidean, having the fundamental unit

$$\epsilon = 1 + \eta \tag{14.2}$$

and having the ring of all algebraic integers equal to

$$\mathfrak{D} = [1, \epsilon] = [1, \eta], \tag{14.3}$$

(which is required in setting up generators of the modular group, as in § 2). In either case,

$$(\eta^2) = (2), \qquad N(\eta) = -2, \tag{14.4}$$

$$\mathfrak{D}_2 = [1, 2\eta] = [1, D^{\frac{1}{2}}]. \tag{14.5}$$

We introduce the simplifying symbol

$$\begin{aligned} e(\zeta) &= \exp \pi i S(\zeta/D^{\frac{1}{2}}) \\ &= \exp \pi i (\zeta - \zeta')/D^{\frac{1}{2}}. \end{aligned} \tag{14.6}$$

In particular,

$$e([r + s\eta]/t) = \exp \pi i s/t; \tag{14.7}$$

thus for the algebraic integer ρ (in $\mathfrak{D}$)

$$(14.8) \qquad e(\rho) = 1 \text{ if and only if } \rho \in \mathfrak{D}_2.$$

Finally, using the complex variables in the argument of $e(\rho)$, we redefine the earlier $\Theta_{d,c}(\tau)$ as follows:

$$(14.9) \qquad \Theta(d, c; \tau) = \sum_{\nu} e(\nu d\eta + [\nu + c\eta/2]^2\tau)$$

summed over all ν in $\mathfrak{D}$, where,

$$(14.10) \qquad \begin{cases} \operatorname{Im}\tau > 0, \\ \operatorname{Im}\tau' < 0. \end{cases}$$

The following transformation laws are determined from formulas:

$$(14.11) \qquad \Theta(d+2, c; \tau) = \Theta(d, c+2; \tau) = \Theta(d, c; \tau),$$

$$(14.12) \qquad \Theta(d, c; \epsilon^2\tau) = \Theta(d, c; \tau),$$

$$(14.13) \qquad \Theta(d, c; \tau + \eta) = \Theta(d+1, c; \tau)e(c^2\eta^3/4),$$

$$(14.14) \qquad \Theta(d, c; \tau + 1) = \Theta(d + c, c; \tau)e(c^2\eta^2/4),$$

$$(14.15) \qquad \Theta(d, c; -1/\tau) = e(cd\eta^2/2)\Theta(c, d; \tau)N(\tau)^{\frac{1}{2}},$$

for the principal square root of $N(\tau)$.

15. Asymptotic relations. To calculate the singular series, we consider $\Theta(d, c; \tau)$ near $\tau = \alpha/\beta$, $(\tau' = \alpha'/\beta')$, an irreducible, algebraic rational in $R(D^{\frac{1}{2}})$.

$$(15.1) \qquad \Theta(d, c; \alpha/\beta + \lambda) = \sum_{\nu} e(\nu d\eta + [\nu + c\eta/2]^2\alpha/\beta)e([\nu + c\eta/2]^2\lambda),$$

where λ, λ' are a new pair of complex variables satisfying condition (14.10). Then, writing

$$(15.2) \qquad \nu = \nu_1 + 2\beta\nu_2, \ (\nu_1 \bmod 2\beta, \nu_2 \text{ arbitrary}),$$

we find

$$(15.3) \qquad \begin{aligned} &\Theta(d, c; \alpha/\beta + \lambda) \\ &\quad = \sum_{\nu_1} e(\nu_1 d\eta + [\nu_1 + c\eta/2]^2\alpha/\beta) \sum_{\nu_2} e([\nu_1 + 2\beta\nu_2 + c\eta/2]^2\lambda). \end{aligned}$$

But the inner sum, according to the general method, is asymptotically independent of ν_1 and c; thus

$$(15.4) \qquad \sum_{\nu_2} \approx \Theta(0, 0, 4\beta^2\lambda) = \Theta(0, 0, -1/(4\beta^2\lambda))/N(4\beta^2\lambda)^{\frac{1}{2}}$$

according to formula (14.9). Finally,

$$(15.5)\qquad \Theta(d,c;\alpha/\beta+\lambda) \approx G_{d,c}(\alpha/\beta)/4\,|N(\beta)|\,N(\lambda)^{\frac{1}{2}},$$

where

$$(15.6)\qquad G_{d,c}(\alpha/\beta) = \sum_{\nu \bmod 2\beta} e(\nu d\eta + (\nu + c\eta/2)^2\alpha/\beta).$$

At this point, we examine the Gaussian-type sum $G_{d,c}(\alpha/\beta)$ more critically and note a new type

$$(15.7)\qquad H_{d,c}(\alpha/\beta) = \sum_{\nu \bmod \beta} e(\nu d\eta + [\nu + c\eta/2]^2\alpha/\beta),$$

when

$$(15.8)\qquad (\alpha + d\eta)(\beta + c\eta) \in \mathfrak{O}_2.$$

Such a sum is characteristic of the cases $D = 8$, 12. In the work of Maass [22, p. 716], no condition like (15.8) arises. Indeed, unless (15.8) is valid, the residues $(\bmod 2\beta)$ ν and $\nu + \beta$ make cancelling contributions to the sum (15.7). Thus, calling $H_{d,c}(\alpha/\beta) = 0$ when (15.8) fails, we have

$$(15.9)\qquad G_{d,c}(\alpha/\beta) = 4H_{d,c}(\alpha/\beta).$$

Finally, changing variables, we say, for τ, τ' near α/β, α'/β',

$$(15.10)\quad \Theta(d,c;\tau) \approx \begin{cases} H_{d,c}(\alpha/\beta)\operatorname{sgn} N(\beta)/N(\beta)^{\frac{1}{2}}N(\beta\tau - \alpha)^{\frac{1}{2}}, \text{ (if } \alpha/\beta \neq 1/0); \\ \delta_{0,c}, \text{ (if } \alpha/\beta = 1/0). \end{cases}$$

(The last item was inserted for completeness. Of course τ, τ' approach infinity consistently with (14.10), and we use the conventional sign and delta function.) The square root will be principal, hence consistent with $\tau \to \infty$, $\tau' \to \infty$ along the positive and negative imaginary axes according to (14.10).

If we compare the asymptotic behaviors as applied to (14.11), (14.12), (14.13), (14.14), we find

$$(15.11)\qquad H_{d+2,c}(\alpha/\beta) = H_{d,c+2}(\alpha/\beta) = H_{d,c}(\alpha/\beta),$$

$$(15.12)\qquad H_{d,c}(\epsilon^2\alpha/\beta) = H_{d,c}(\alpha/\beta),$$

$$(15.13)\qquad H_{d,c}(\alpha/\beta + \eta) = e(c^2\eta^3/4)H_{d+1,c}(\alpha/\beta),$$

$$(15.14)\qquad H_{d,c}(\alpha/\beta + 1) = e(c^2\eta^2/4)H_{d+c,c}(\alpha/\beta),$$

which incidentally could be verified from (15.7). A more difficult result is the *reciprocity*:

(15.15) $$H_{c,d}(\alpha/\beta)/N(\beta)^{\frac{1}{2}} = \operatorname{sgn}(\alpha,\beta)\,(H_{d,c}(-\beta/\alpha)/N(\alpha)^{\frac{1}{2}})\,e(cd\eta^2/2).$$

Here

(15.16) $$\begin{cases} \operatorname{sgn}(\alpha,\beta) = -1 \text{ with the following arrays:} \\ \quad \begin{matrix} \alpha & \alpha' & \beta & \beta' \\ \pm & \pm & \mp & \pm \\ - & + & \pm & \pm \end{matrix} \\ \operatorname{sgn}(\alpha,\beta) = +1, \text{ otherwise.} \end{cases}$$

The reciprocity relation (15.16) is proved by the Cauchy-Hecke method of comparing (15.10) with

(15.17) $$\Theta(c,d;\sigma) \approx H_{c,d}(-\beta/\alpha)\operatorname{sgn} N(\alpha)/N(\alpha)^{\frac{1}{2}}N(\alpha\sigma+\beta)^{\frac{1}{2}}$$

using (14.15) under the comparison $\sigma\tau = -1$. The details are very similar to Hecke [18] except that we permit $N(\alpha)^{\frac{1}{2}}$ to be imaginary, thereby forcing the "balancing" factor, $\operatorname{sgn}(\alpha,\beta)$, to be real.

By virtue of identities (15.11) through (15.14) we can confine all our attention to $H_{0,0}(\alpha/\beta)$ henceforth abbreviated:

(15.18) $$H_{0,0}(\alpha/\beta) = H(\alpha/\beta) = \sum_{\nu \bmod \beta} e(\nu^2\alpha/\beta).$$

Unless

(15.19) $$\alpha\beta \in \mathfrak{D}_2,$$

we note $H(\alpha/\beta)$ is trivially taken as 0.

16. Hecke's modular function. The superposition of the elements (15.10) for $\Theta^k(d,c;\tau)$ does not create an absolutely convergent series until $k > 4$. To remedy this fact, Hecke created the series with convergence factor:

(16.1) $$\Psi(d,c;\tau;k,s) = \delta_{0,c} + \sum_{\alpha/\beta} H^k_{d,c}(\alpha/\beta)\operatorname{sgn}^k N(\beta)/N(\beta)^{k/2}N(\beta\tau-\alpha)^{k/2}\,|N(\beta\tau-\alpha)|^s.$$

Our interest shall center about $k = 3$, but the general integer k is momentarily useful. This series converges when

(16.2) $$k/2 + \operatorname{Re} s > 2.$$

(We shall be spared the tedium of repeating the convergence majorants by virtue of the similarity with estimates valid for $D = 5$; see [21].)

By virtue of the relations (15.11) through (15.15) we find, omitting symbols k, s when convenient,

(16.3) $$\Psi(d,c;\tau) = \Psi(d+2,c;\tau) = \Psi(d,c+2;\tau),$$

$$(16.4)\qquad \Psi(d, c; \epsilon^2\tau) = \Psi(d, c; \tau),$$

$$(16.5)\qquad \Psi(d, c; \tau + \eta) = \Psi(d, c; \tau)\, e^k(c^2\eta^2/4),$$

$$(16.6)\qquad \Psi(d, c; \tau + 1) = \Psi(d + c, c; \tau)\, e^k(c^2\eta^2/4),$$

$$(16.7)\qquad \Psi(d, c; -1/\tau) = \Psi(c, d; \tau)\, e^k(cd\eta^2/2) N(\tau)^{k/2} \,|\, N(\tau) \,|^s.$$

Hecke's work [7] shows that the function Ψ has no finite singularities in s, hence by analytic continuation we can let $s = 0$. In so doing, we obtain a function Ψ satisfying the same functional equations as Θ^k. The significance of this fact we leave until later on. Most important for computational purposes is the fact that the series (16.1) is susceptible to a fortuitous arrangement before making $s = 0$. Again we spare the reader the details on majorants, by referring to the similar case where $D = 5$.

It suffices to restrict ourselves to the case $d = 0$, $c = 0$ and simply write

$$(16.8)\qquad \Psi(\tau) = \Psi(0, 0; \tau; k, s).$$

17. Rearrangement of series. We first write

$$(17.1)\qquad \Psi(\tau) = 1 + \sum_{\substack{\alpha/\beta \bmod 2 \\ \alpha\beta \in \mathfrak{O}_2}} (H^k(\alpha/\beta)/|\, N(\beta) \,|^{k+s}) \Phi(\alpha/\beta, \tau),$$

where

$$(17.2)\qquad \Phi(\alpha/\beta, \tau) = \sum_{\nu} N(\tau - \alpha/\beta + 2\nu)^{-k/2} \,|\, N(\tau - \alpha/\beta + 2\nu) \,|^{-s}.$$

(Note that the $\operatorname{sgn}^k N(\beta)$ of (16.1) disappears when $N(\beta)$ is divided out.) By making use of the Poisson-Lipschitz formula, again, we find

$$(17.3)\qquad \Phi(\alpha/\beta, \tau)$$

$$= (1/4D^{\frac{1}{2}}) \sum_{\mu} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e(-P\mu)\, dP dP' / N(P - \alpha/\beta + \tau)^{k/2} \,|\, N(P - \alpha/\beta + \tau) \,|^s,$$

where P and P' are real variables and μ is summed over $\mathfrak{O}$. Introducing, with Hecke,

$$(17.4)\qquad B(\mu, \tau) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e(-P\mu)\, dP dP' / N(P + \tau)^{k/2} \,|\, N(P + \tau) \,|^s,$$

we find the singular series

$$(17.5)\qquad \Psi(\tau) = 1 + \sum_{\mu} (B(\mu, \tau)/2D^{\frac{1}{2}}) P(\mu),$$

where

$$(17.6)\qquad P(\mu) = \sum_{\substack{\alpha/\beta \bmod 2 \\ \alpha\beta \in \mathfrak{O}_2}} H^k(\alpha/\beta) e(-\mu\alpha/\beta)/2 \;|\, N(\beta) \,|^{k+s}.$$

Now we know, in advance, that only totally positive μ can be present in $\mathfrak{S}^k$, (although other μ are present before we set $s = 0$). We can see more clearly that all μ entering into (17.5) are in $\mathfrak{D}_2$, for, by (15.14),

$$(17.7) \qquad H(\alpha/\beta + 1) = H(\alpha/\beta);$$

but $e(-\mu[\alpha/\beta + 1]) = -e(-\mu\alpha/\beta)$ if $\mu \notin \mathfrak{D}_2$.

We next introduce the symbol

$$(17.8) \quad P(\beta,\mu) = \sum_{\substack{\alpha \bmod \beta, (\alpha,\beta)=1 \\ \alpha\beta \in \mathfrak{D}_2}} H^k(\alpha/\beta) e(-\mu\alpha/\beta) + H^k((\alpha + \beta\eta)/\beta) e(-\mu[\alpha + \beta\eta]/\beta),$$

aware that $H(\alpha^*/\beta^*) = 0$ if $\alpha^*\beta^* \notin \mathfrak{D}_2$. Then we find

$$(17.9) \qquad P(\mu) = \sum_{(\beta)} P(\beta,\mu)/|N(\beta)|^{k+s}.$$

The remarkable simplification now achieved is due entirely to the fact that if $(\beta_1, \beta_2) = 1$,

$$(17.10) \qquad H(\alpha/\beta_1\beta_2) = H(\alpha_1/\beta_1)H(\alpha_2/\beta_2) \text{ for special } \alpha_1, \alpha_2,$$

$$(17.11) \qquad P(\beta_1,\mu) \cdot P(\beta_2,\mu) = P(\beta_1\beta_2,\mu).$$

A corresponding result was proved by Maass [22; p. 736] using a Lemma of Siegel. Actually, a direct proof (like the one in the case of elementary Gaussian sums [20]) can work if we strictly observe that we must have $\alpha\beta \in \mathfrak{D}_2$, in our choice of α_1 and α_2 in (17.10).

Thus if we list the prime divisors in $R(D^{\frac{1}{2}})$, denoted by $\mathfrak{p}$, we find, by unique factorization,

$$(17.12) \qquad P(\mu) = \prod_{\mathfrak{p}} P_{\mathfrak{p}}(\mu),$$

where,

$$(17.13) \qquad P_{\mathfrak{p}}(\mu) = 1 + \sum_{t=1}^{\infty} P(\mathfrak{p}^t,\mu)/|N(\mathfrak{p})|^{t(k+s)}.$$

On the other hand, as $s \to 0$, when $\mu \gg 0$,

$$(17.14) \qquad B(\mu,\tau) \to [4N(\mu)^{k/2-1}\pi^k/D^{k/2-1}\Gamma^2(k/2)]\, e(\mu\tau)$$

by use of the Γ-integral. Thus, making use of uniform convergence majorants [21] as $s \to 0$, we find, when $k = 3$

$$(17.15) \qquad \begin{cases} \Psi(\tau) = \sum\limits_{0 \ll \mu \in \mathfrak{D}_2} e(\mu\tau) Z(\mu), \\ Z(\mu) = 8\pi^2 P(\mu)\, (N(\mu)/D^2)^{\frac{1}{2}}. \end{cases}$$

We have to next show $\Theta^8 = \Psi$ and then to simplify $P(\mu)$ to the point where it is recognizable. We do the latter first.

Quadratic Residue Properties.

18. Basic formulas. It is apparent, by now, that we can deduce most of the results on $H(\alpha/\beta)$ by analogy with Gaussian sums. We can, of course, restrict ourselves to β a prime power.

First we take π an *odd* prime in $R(D^{\frac{1}{2}})$, $(\pi) \neq (\eta)$. We note $\pi = q$ if $(D/q) = -1$, for q a rational prime and $\pi\pi' = p$ if $(D/p) = 1$, for p a rational prime. We now standardize π by the condition $\pi \in \mathfrak{O}_2$, at least to within the factor $\pm \epsilon^{2u}$, (u integral), (by choosing $\epsilon\pi$ if $\pi \notin \mathfrak{O}_2$). Thus, for $D = 8$, $\pi = 3, 5, 1 \pm 2 \cdot 2^{\frac{1}{2}}, 11, 13, 5 \pm 2 \cdot 2^{\frac{1}{2}}, \cdots$, etc. For $D = 12$, $\pi = 3 + 2 \cdot 3^{\frac{1}{2}}, 5, 7, 1 \pm 2 \cdot 3^{\frac{1}{2}}, 5 \pm 2 \cdot 3^{\frac{1}{2}}$, etc. (Note, $(3 - 2 \cdot 3^{\frac{1}{2}}) = -(3 + 2 \cdot 3^{\frac{1}{2}})\epsilon^{-2}$.) The primes, of course, will not necessarily have positive norm.

Next we observe a "polygon" theorem:

$$(18.1) \qquad \sum_{\zeta \bmod \beta} e(2\zeta\alpha/\beta) = \begin{cases} |N(\beta)| & \text{if } \alpha/\beta \text{ is an integer,} \\ 0 & \text{otherwise.} \end{cases}$$

The proof consists of showing if α/β is no integer, the sum is unchanged by multiplication by $e(2\zeta_0\alpha/\beta)$, ($\neq 1$ for a properly chosen ζ_0). Using this, we consider

$$(18.2) \qquad H(\alpha/\pi^t) = \sum_{\nu \bmod \pi^t} e(\nu^2\alpha/\pi^t), \qquad \alpha \in \mathfrak{O}_2,$$

We set $\nu = \pi^{t-1}\nu_1 + \nu_2$, ($\nu_1 \bmod \pi$, $\nu \bmod \pi^{t-1}$), and we discover

$$H(\alpha/\pi^t) = \sum_{\nu_2 \bmod \pi^{t-1}} e(\nu_2{}^2\alpha/\pi^t) \sum_{\nu_1 \bmod \pi} e(2\nu_1\nu_2\alpha/\pi),$$

$$(18.3) \qquad H(\alpha/\pi^t) = |N(\pi)|\, H(\alpha/\pi^{t-2}), \qquad \alpha \in \mathfrak{O}_2, t \geqq 2.$$

Since $H(\alpha) = 1$, trivially, we concentrate on $H(\alpha/\pi)$.

We next distinguish the quadratic residues mod π by introducing the symbol

$$(18.4) \qquad (\lambda/\pi) = \begin{cases} 1 & \text{if } \lambda \equiv \xi^2 \bmod \pi, (\lambda, \pi) = 1, \\ -1 & \text{if } \lambda \not\equiv \xi^2 \bmod \pi, (\lambda, \pi) = 1, \\ 0 & \text{if } (\lambda, \pi) \neq 1. \end{cases}$$

Then if we consider ρ the residues mod π, $(\rho/\pi) = 1$, and ν the non-residues mod π, $(\nu/\pi) = -1$, we form

$$(18.5) \qquad \begin{cases} R = \sum e(\rho/\pi), \\ N = \sum e(\nu/\pi), \end{cases}$$

since we can easily make $\rho \in \mathfrak{O}_2$ (by adding $\pi\epsilon$). Clearly

$$H(1/\pi) = 1 + 2R, \tag{18.6}$$

$$0 = 1 + R + N, \tag{18.7}$$

the latter following if we select ρ and ν from the complete set of residues 2ζ, (ζ varying mod π), using (18.1). Thus, as in the Gaussian case,

$$H(1/\pi) = R - N = \sum(\alpha/\pi)e(\alpha/\pi), \tag{18.8}$$

$$H(\alpha/\pi) = (\alpha/\pi)H(1/\pi), \text{ if } \alpha \in \mathfrak{O}_2 \tag{18.9}$$

We now need to evaluate only $H(1/\pi)$. By quadratic reciprocity (15.15);

$$H(1/\pi)/N(\pi)^{\frac{1}{2}} = \operatorname{sgn}(1,\pi)H(-\pi/1)/1 = \operatorname{sgn}(1,\pi). \tag{18.10}$$

Hence, for odd t,

$$H(\alpha/\pi^t) = \{(\alpha/\pi)\operatorname{sgn}(1,\pi)\}^t \,|N(\pi)|^{t/2}\{\operatorname{sgn} N(\pi)\}^{\frac{1}{2}}, \tag{18.11a}$$

while, for even t,

$$H(\alpha/\pi^t) = |N(\pi)|^{t/2}. \tag{18.11b}$$

Next take the even prime, η. For $\beta = \eta^t$, we find that the expression $H(\alpha/\beta)$ makes sense, with $(\alpha, \beta) = 1$, exactly when $t \geqq 2$. Even so, using the polygon theorem (18.1), we find by an argument similar to the one in the last section,

(18.12) $H(\alpha/\eta^t) = 2H(\alpha/\eta^{t-2})$ if $t \geqq 4$. Here α need not belong to $\mathfrak{O}_2$. Thus every value of $H(\alpha/\eta^t)$ can be computed directly from these:

$$\begin{cases} H(1/\eta^2) = 2;\ H(1/\eta^3) = 2\cdot 2^{\frac{1}{2}}i, \\ H((1+\eta)/\eta^2) = \begin{pmatrix} 2i \\ 2 \end{pmatrix},\ H(3/\eta^3) = 2\cdot 2^{\frac{1}{2}}i, \\ H((1+\eta)/\eta^3) = \begin{pmatrix} 2\cdot 2^{\frac{1}{2}} \\ 2\cdot 2^{\frac{1}{2}}i \end{pmatrix},\ H((3+\eta/\eta^3) = \begin{pmatrix} -2\cdot 2^{\frac{1}{2}} \\ -2\cdot 2^{\frac{1}{2}}i \end{pmatrix}. \end{cases} \tag{18.13}$$

In cases where two values $\begin{pmatrix} \cdots \\ \cdots \end{pmatrix}$ are bracketed, the upper one belongs to $D = 8$ and the lower one belongs to $D = 12$.

We also note the further results:

$$H(\alpha/\eta^t + \eta) = H(\alpha/\eta^t), \qquad t \geqq 4, \tag{18.14}$$

$$H(\alpha/\eta^2 + \eta) = H(\alpha/\eta^2)e(\alpha), \tag{18.15}$$

$$H(\alpha/\eta^3 + \eta) = -H(\alpha/\eta^3). \tag{18.16}$$

The first follows from the observation that in the sum (15.18) for $H(\alpha/\eta^t)$ only the even ν enter, the odd ν cancel out to make possible (18.12).

By formula (17.10) we can show, finally,

$$|H(\alpha/\beta)| = |N(\beta)|^{\frac{1}{2}} \tag{18.17}$$

if $\alpha\beta \in \mathfrak{O}_2$ and α/β is reduced.

19. Quadratic reciprocity. The epitome of the theory is the deduction of quadratic reciprocity by the method of Hecke. Our principal variation consists in the restriction $\alpha\beta \in \mathfrak{O}_2$, in $H(\alpha/\beta)$.

If π_1 and π_2 are odd primes in $\mathfrak{O}_2$ by using (15.15), (18.9), and (18.10):

$$(\pi_1/\pi_2)(\pi_2/\pi_1) = \{\pi_1, \pi_2\}, \tag{19.1}$$

where $\{\pi_1/\pi_2\} = \operatorname{sgn}(1, \pi_1)\operatorname{sgn}(1, \pi_2)\operatorname{sgn}(\pi_1, \pi_2)\operatorname{sgn} N(\pi_1)$, or

$$\left\{\begin{array}{l} \{\pi_1, \pi_2\} = -1 \text{ under the array of signs:} \\ \pi_1 \;\; \pi_1' \;\; \pi_2 \;\; \pi_2' \\ \pm \;\; \mp \;\; \pm \;\; \mp, \;\; \pi_1\pi_2 \gg 0; N(\pi_1) < 0, N(\pi_2) < 0; \\ \pm \;\; \mp \;\; - \;\; -, \;\; \pi_2 \ll 0; N(\pi_1) < 0; \\ - \;\; - \;\; \pm \;\; \mp, \;\; \pi_1 \ll 0; N(\pi_2) < 0; \\ \{\pi_1, \pi_2\} = +1, \text{ otherwise.} \end{array}\right. \tag{19.2}$$

Then the first completion theorem also emerges in the process:

$$(-1/\pi) = \operatorname{sgn} N(\pi). \tag{19.3}$$

We can deduce the rational results: If $\pm p$ denotes $\pi\pi'$, $p > 0$, then $\xi^2 + 1 \equiv 0 \bmod \pi$ is solvable exactly when $x^2 + 1 \equiv 0 \bmod p$ is solvable. This implies, in rational symbols, $(D/p) = (-1/p) = +1$, hence $p \equiv 1 \bmod D$ for $D = 8$ and 12. Thus the elementary theory of quadratic forms yields the following expression, for an arbitrary $p \equiv 1 \pmod 8$:

$$p = u_1^2 - 8v_1^2 = N(\pi_1), \qquad \pi_1 = u_1 + 2 \cdot 2^{\frac{1}{2}} v_1, \tag{19.4}$$

and one (not both) of the following for $p \equiv 1 \pmod{12}$:

$$p = \left\{\begin{array}{l} u_2^2 - 12v_2^2 = N(\pi_2), \;\; \pi_2 = u_2 + 2 \cdot 3^{\frac{1}{2}} v_2, \\ 4u_3^2 - 3v_3^2 = N(\pi_3), \;\; \pi_3 = 2u_3 + 3^{\frac{1}{2}} v_3. \end{array}\right. \tag{19.5}$$

Clearly, π_1, π_2, and $(2 + 3^{\frac{1}{2}})\pi_3$ all $\in \mathfrak{O}_2$, verifying (19.3). Conditions (19.4) and (19.5) are clearly necessary and sufficient for $(-1/\pi) = 1$, when π is not a rational prime.

A less simple case is the second completion theorem. We apply the reciprocity formula (15.15) to $H(\eta^3/-\pi)$ and obtain a set of values of

$(\eta/-\pi)$ as related to $H(+\pi/\eta^3)$, which is determined by $\pi \pmod{2\eta^3}$, (not $\bmod\,\eta^3$, by (18.16)). Since the steps are finite in number, we omit tedious details:

$$(19.6)\qquad (\eta/\pi) = \operatorname{sgn}(1,-\pi)\operatorname{sgn}(\eta^3,-\pi)H(\pi/\eta^3)/2\ 2^{\frac{1}{2}}, \qquad (\pi \in \mathfrak{O}_2).$$

Thus from formulas (18.13) and (18.16) for $D = 8$ or 12:

$$(19.7)\qquad (\eta/\pi) = \begin{cases} +\operatorname{sgn}\pi' \text{ if } \pi \equiv 1, 1+\eta^3, 3, 3+\eta^3 \pmod{4\eta}, \\ -\operatorname{sgn}\pi' \text{ if } \pi \equiv 5, 5+\eta^3, 7, 7+\eta^3 \pmod{4}. \end{cases}$$

The final completion law is found by doing likewise with $H(\epsilon\eta^3/-\pi)$ and finding $(\epsilon\eta/\pi)$. Omitting details, we note

$$(19.8)\qquad (\epsilon\eta/\pi) = \operatorname{sgn}(1,-\pi)\operatorname{sgn}(\epsilon\eta^3,-\pi)H(\pi/\epsilon\eta^3)/2\ 2^{\frac{1}{2}}[-N(\epsilon)]^{\frac{1}{2}}, \qquad (\pi \in \mathfrak{O}_2).$$

Thus, as before, with ϵ defined in (14.2), we find the remarkable result for $D = 8$, $\pi \in \mathfrak{O}_2$,

$$(19.9)\qquad (\epsilon/\pi) = \operatorname{sgn}\pi' \text{ if } \pi \equiv 1, 3+2\eta \qquad \pmod{4},$$

$$(19.10)\qquad (\epsilon/\pi) = -\operatorname{sgn}\pi' \text{ if } \pi \equiv 1+2\eta, 3 \qquad \pmod{4},$$

and for $D = 12$, $\pi \in \mathfrak{O}_2$,

$$(19.11)\qquad (\epsilon/\pi) = 1 \text{ if } \pi \equiv 1, 3 \qquad \pmod{4},$$

$$(19.12)\qquad (\epsilon/\pi) = -1 \text{ if } \pi \equiv 1+2\eta, 3+2\eta \qquad \pmod{4}.$$

We note that lines (19.10) and (19.11) represent the odd residue classes for which $\pi \equiv -\xi^2 \bmod 4$. The pattern emerges again for the table in § 12 (above).

20. The zeta series. We next consider the various series $P\mathfrak{p}(\mu)$, starting with $P(\mathfrak{p}^t, \mu)$, of § 17.

If π is odd, in expression (17.8) for $P(\pi^t, \mu)$ we note if α and $\pi \in \mathfrak{O}_2$, then we have simply (for $k = 3$),

$$(20.1)\qquad \begin{aligned} P(\pi^t,\mu) &\sum_{\substack{\alpha \bmod \pi^t \\ (\alpha,\pi)=1}} H^3(\alpha/\pi^t)e(-\mu\alpha/\pi^t), \qquad t \geqq 1) \\ &= |N(\pi)|^{3t/2}[\operatorname{sgn}^t N(\pi)]^{3/2}\operatorname{sgn}^t(1,\pi) \sum_{\alpha \bmod \pi^t} (\alpha/\pi)^t e(-\mu\alpha/\pi^t). \end{aligned}$$

The inner sum is recognizable again as a character sum, not unlike (18.8), except for the fact that π could divide μ. Let us write

$$(20.2)\qquad \mu = \pi^m\mu^* \qquad (\mu^*, \pi) = 1, \qquad (m \geqq 0),$$

then we find after an elaborate effort:

$$(2.3)\quad P(\pi^t,\mu)=\begin{cases} \left.\begin{array}{ll} 0 & t \text{ odd} \\ |N(\pi)|^{5/2}(1-1/|N(\pi)|) & t \text{ even} \end{array}\right\} 1 \leqq t \leqq m, \\ \left.\begin{array}{ll} |N(\pi)|^{(5t-1)/2}(-\mu^*/\pi) & t \text{ odd} \\ -|N(\pi)|^{5t/2-1} & t \text{ even} \end{array}\right\} t=m+1, \\ \quad 0 \qquad\qquad\qquad t>m+1. \end{cases}$$

The interesting cases are where μ is square-free so $m=0$ or 1. In either case, following a familiar pattern [12, p. 190]

$$(20.4)\qquad P_\pi(\mu)=(1-|N(\pi)|^{-2-2s})/(1-(-\mu/\pi)|N(\pi)|^{-1-s}),\quad \pi\neq\eta.$$

The contribution of η is more complicated. First of all, the analogue of (20.1) is the more complex expression

$$(20.5)\qquad \begin{aligned} P(\eta^t,\mu)=\sum_{\substack{\alpha(\operatorname{mod}\eta^t)\\(\alpha,\eta)=1}} & H^3(\alpha/\eta^t)e(-\mu\alpha/\eta^t) \\ & +H^3(\alpha/\eta^t+\eta)e(-\mu\alpha/\eta^t-\mu\eta). \end{aligned}$$

We therefore see that if μ is odd, $\mu\in\mathfrak{O}_2$, by (18.14), $P(\eta^t,\mu)\equiv 0$ if $t\geqq 4$. The problem is then finitary and details can be omitted. We introduce the characters

$$(20.6)\qquad Q(-\mu,\epsilon)=\begin{cases} 1 \text{ if } -\mu\equiv\xi^2 \bmod 4, \\ -1 \text{ if } -\mu\not\equiv\xi^2 \bmod 4. \end{cases}$$

(Clearly $Q=-1$ necessarily if $\mu\notin\mathfrak{O}_2$). Since $\mu\gg 0$, this character is consistent with (19.9), etc., (if $\pi=-\mu$ formally). We introduce the further character,

$$(20.7)\qquad Q(-\mu,\eta)=\begin{cases} 1 \text{ if } -\mu\equiv\xi^2 \pmod{4\eta},\ \mu \text{ odd}; \\ -1 \text{ if } -\mu\not\equiv\xi^2 \pmod{4\eta} \text{ but } -\mu\equiv\xi^2 \pmod 4,\ \mu \text{ odd}; \\ 0 \text{ if } -\mu\not\equiv\xi^2 \bmod 4, \text{ or } (\mu,\eta)\neq 1. \end{cases}$$

The characters $Q(-\mu,\epsilon)$ and $Q(-\mu,\eta)$ are like the rational characters $(-1/p)$ and $(p/2)$.

Now we can verify that if μ is square-free, and $\mu\gg 0$, $\mu\in\mathfrak{O}_2$,

$$(20.8)\qquad P(\eta^2,\mu)=16Q(-\mu,\epsilon),$$

$$(20.9)\qquad P(\eta^3,\mu)=128Q(-\mu,\eta),$$

so that for $\mu\in\mathfrak{O}_2$, square-free, totally positive, $P_\eta(\mu)=P_0(\mu)$, where

$$(20.10)\qquad P_0(\mu)=1+Q(-\mu,\epsilon)/4\ \ 2^{2s}+Q(-\mu,\eta)/4\ \ 2^{3s}.$$

We more generally consider $\mu\gamma^2$ defined according to (12.3) to cover cases where $\mu\notin\mathfrak{O}_2$. Then it can be seen

$$(20.11)\qquad P_\eta(\mu\gamma^2) = P_0(\mu).$$

We consider terms of the special type with coefficient defined as shown:

$$(20.12)\qquad \Psi(\tau) = \sum e(\mu\gamma^2\tau)Z(\mu\gamma^2) + \cdots.$$

We then make a series of substitutions to obtain a convenient formula for $Z(\mu\gamma^2)$. The details are lengthy, but we might just dwell on properties of the field $R(D^{\frac12}, (-\mu)^{\frac12})$ as a relative quadratic field over $R(D^{\frac12})$. Thus the zeta function

$$(20.13)\qquad \prod_{\pi}(1-|N(\pi)|^{-2})^{-1} = 16\pi^4 C/D^{3/2},\quad (C_8 = 1/48, C_{12} = 1/24),$$

from § 5. We also note the relative zeta function [18] for the adjunction of $(-\mu)^{\frac12}$ to $R(D)^{\frac12}$ is

$$(20.14)\qquad \begin{aligned}&\prod_{\pi\,\mathrm{odd}}(1-(-\mu/\pi)/|N(\pi)|)^{-1}\cdot(1-Q(-\mu,\eta)/2)^{-1}\\ &\qquad = H(D^{\frac12}, -\mu)^{\frac12})\,(2\pi^2/w)/(\log|\epsilon|/\log|E|)\,(\Delta/D)^{\frac12},\end{aligned}$$

where Δ is the discriminant of $R(D^{\frac12}, (-\mu)^{\frac12})$, w is the number of complex roots of unity and E is the fundamental unit of this larger field. We can now write, if we let $s \to 0$, in the terminology of (12.2),

$$(20.15)\qquad Z(\gamma^2\mu) = H(D^{\frac12}, (-\mu)^{\frac12})\,G$$

where, for square-free, totally positive μ,

$$(20.16)\qquad G = \frac{\left\{1 + \dfrac{Q(-\mu,\epsilon)}{4} + \dfrac{Q(-\mu,\eta)}{4}\right\}\ (4/3)\left\{1 - \dfrac{Q(-\mu,\eta)}{2}\right\}\ (2/w)}{C_D(\Delta/N(\mu\gamma^2)D^2)^{\frac12}\ \dfrac{\log|\epsilon|}{\log|E|}}$$

This is substantially the G of (12.2), if we find Δ according to the usual theory of relative-quadratic fields. Referring to (20.6), the relative basis is (for $D = 8, 12$),

$$(20.17)\qquad \begin{cases}[1, (\xi + (-\mu)^{\frac12})/2], & \text{if } Q(-\mu,\epsilon) = 1,\\ [1, (1 + (-\mu)^{\frac12})/\eta], & \text{if } Q(-\mu,\epsilon) = -1,\ \mu \in \mathfrak{O}_2,\\ [1, (-\mu)^{\frac12}], & \text{if } \mu \notin \mathfrak{O}_2.\end{cases}$$

Of course, in the first two cases $\gamma = 1$, while in the third $N(\gamma) = 2$. To complete the explanation, we might add that $w = 2$ and $|\epsilon| = |E|$ except in cases cited in (12.4), which we exclude.

As a concluding remark to this section we observe that the progress from formulae (17.12-17.15) to (20.15) depends heavily on Gaussian sum manipulations. Here many details were not needed, particularly those typified by the reduction of such sums to "normal form" and the use of the "zero-rule," as, for example, in Hasse's work [16a; p. 14]. The zeta-function manipulations, however, are still best derived as *ad hoc* extensions of Maass' work [12]; while the identification of the modular forms will be done by a more direct method, starting in § 22 below.

21. Singular series for four squares. Before proceedings to the proof that $\Theta^3 = \Psi$, we note in retrospect how the singular series could be developed for the fourth power. In the earlier paper, [16], formula (51a) yields, essentially, for $D = 8, 12$, that the singular series for $\Theta_{0,0}(\tau)$ is

$$\Omega_{0,0}(\tau) = \{4A_1(\tau) + 64A_0(4\tau) + 4A_0(\tau) - 24A_0(2\tau)\}C_D' + 1 \tag{21.1}$$

where

$$\begin{cases} A_\kappa(\tau) = \lim\limits_{s\to\infty} \sum [N(\nu\tau+\mu)]^{-2}\,|N(\nu\tau+\mu)|^{-s}, \\ \quad \nu\kappa \equiv \mu, \pmod 2, \\ \quad (\nu) \neq (0), \end{cases} \tag{21.2}$$

and

$$C_D' = D^{3/2}/48\pi^4 C_D. \tag{21.3}$$

It is no great difficulty to evaluate the singular series (16.1) for $k = 4$ and obtain the matching series

$$\Psi(0,0;\tau;4,s) = 1 + \sum_{\alpha/\beta,\,\alpha\beta\in\mathfrak{O}_2} [N(\beta\tau-\alpha)]^{-2}\,|N(\beta\tau-\alpha)|^{-s}. \tag{21.4}$$

This can best be done using formulas (17.10), (18.11), (18.13), which assures us

$$H^4(\alpha/\beta) = N(\beta)^2. \tag{21.5}$$

We pause here to note that the summation condition "$\alpha\beta \in \mathfrak{O}_2$ for α/β reduced" actually encompasses the rather complicated coefficients in (21.1). In fact, examining Götzky's work equally critically we note, for $D = 5$,

$$[\sum e(\nu^2\tau)]^4 = \{8A_0(\tau) + 128A_0(4\tau) - 16A_0(2\tau)]D^{3/2}/\pi^4 + 1. \tag{21.6}$$

Again, this fairly complicated expression of Götzky could have been written as (21.4), $(s \to 0)$, with the restriction α/β be reduced and α and β not be both odd. (The last restriction, of course, enters Jacobi's well-known demonstration involving four *rational* squares.)

Equality of Theta Series and Singular Series.

22. Modular forms. The functions $\Psi(d,c;\tau,3,0)$ and $\Theta^3(d,c;\tau)$ satisfy the same functional equations (14.11)-(14.15) and (16.3)-(16.7). Are they proportional?

We revert to the procedure of § 7. We note that $\Theta(d,c;\tau)$ can vanish, within its functional domain, only on a well defined zero-manifold. This manifold exists only for $d=c=1$ and is the complex (two dimensional) manifold

$$v=0 \tag{22.1}$$

in new complex cooridnates (u,v) defined as follows:

$$\begin{cases} \tau=-\epsilon' u+v, \\ \tau'=-\epsilon u+v, \text{ for } D=8; \end{cases} \tag{22.2}$$

$$\begin{cases} \tau=u+v, \\ \tau'=-u+v, \text{ for } D=12. \end{cases} \tag{22.3}$$

Furthermore, on this manifold, the zeros are simple, (see § 7), or,

$$\partial\Theta(u,v)/\partial v\neq 0 \text{ for all } u, \text{ (at } v=0). \tag{22.4}$$

We need only show that $\Psi(d,c;\tau,3,0)/\Theta^3(d,c,\tau)$ has no poles in the fundamental domain by establishing a third order zero for Ψ when $d=c=1$ and $v=0$. We can draw our conclusion (that Ψ and Θ^3 are proportional) from Theorem 4 (§ 2).

We define $\Xi(d,c;\tau)$ as a system of four modular functions (as d, c vary) in τ and τ', having no finite singularities and satisfying the system (16.3)-(16.7) with $k=3$, (dimension $-3/2$), and $s=0$. Then we conclude

$$\begin{cases} \Xi(1,1,-\epsilon'^2/\tau^2)=\Xi(1,1,\tau)N(\tau)^{3/2}, \\ \Xi(1,1,\tau-\epsilon')=-i\Xi(1,1,\tau), \text{ for } D=8; \end{cases} \tag{22.5}$$

$$\begin{cases} \Xi(1,1,-1/\tau)=\Xi(1,1,\tau)N(\tau)^{3/2}, \\ \Xi(1,1,\tau+\eta-1)=-\Xi(1,1,\tau), \text{ for } D=12. \end{cases} \tag{22.6}$$

We next define

$$\begin{cases} \Gamma(u,v)=\Xi(1,1;\tau)=\Xi(1,1;\tau,\tau'), \\ \Gamma_t(u)=(\partial/\partial v)^t\Gamma(u,v) \text{ at } v=0. \end{cases} \tag{22.7}$$

Then let j denote the integer $\geqq 0$, for which

$$\Gamma_0(u)\equiv\Gamma_1(u)\equiv\cdots\equiv\Gamma_j(u)\equiv 0;\ \Gamma_{j+1}(u)\not\equiv 0. \tag{22.8}$$

Then since $N(\tau)=-u^2$, on the zero manifold while $\partial/\partial v=\partial/\partial\tau+\partial/\partial\tau'$, etc., for $t\leqq j$,

$$(22.9)\qquad \begin{cases} \Gamma_t(u+1) = -i\Gamma_t(u), \\ \Gamma_t(-1/u) = -i\Gamma_t(u)u^{2t+3}, \\ \Gamma_t(u) \to 0, \text{ as } u \to i\infty, \text{ for } D = 8; \end{cases}$$

$$(22.10)\qquad \begin{cases} \Gamma_t(u+3^{\frac{1}{2}}) = -\Gamma_t(u), \\ \Gamma_t(-1/u) = -i\Gamma_t(u)u^{2t+3}, \\ \Gamma_t(u) \to 0, \text{ as } u \to i\infty, \text{ for } D = 12. \end{cases}$$

If we could show $j \geqq 3$, we shall then have established that $\psi = \mathfrak{G}^3$. We can do this only for $D = 8$ (and with an additional bit of special information, distinguishing this case from $D = 12$, as we now develop).

23. Special Fourier expansions. We first shall estimate the order of magnitude of $\Gamma_t(u)$ as $u \to \infty$. To do this we expand $\psi(1,1;\tau;k,s)$ by the Poisson-Lipschitz formula as in § 17. The only difference is that, whereas earlier $H(\alpha/\beta) = H_{0,0}(\alpha/\beta) = H_{0,0}(\alpha/\beta + 2\nu)$, now we must use

$$(23.1)\qquad H_{1,1}(\alpha/\beta + 2\nu) = e(\nu\eta^2/2)H_{1,1}(\alpha/\beta)$$

Thus we must insert the factor $e(\nu\eta^2/2)$ into the numerator of the fraction in the summation of (17.2). This produces the result (in contrast to (17.15)),

$$(23.2)\qquad \Psi(1,1;\tau,3,s) = \sum_{\mu^* \gg 0} e(\mu^*\tau)8\pi^2 P^*(\mu)(N(\mu^*)D^{-2})^{\frac{1}{2}},$$

where

$$(23.3)\qquad \mu^* = \mu + \tfrac{1}{2}\cdot\eta^2/2, \qquad \mu \in \mathfrak{O}_2,$$

and

$$(23.4)\qquad P^*(\mu^*) = \tfrac{1}{2}\sum_{\alpha/\beta \bmod 2} H^3{}_{1,1}(\alpha/\beta)e(-\mu^*\alpha/\beta)\,|\,N(\beta)\,|^{-(k+s)}$$

where $H_{1,1}$ has meaning, of course, only when

$$(23.5)\qquad (\alpha+\eta)(\beta+\eta) \in \mathfrak{O}_2.$$

We now have to separate the cases: When $D = 8$, we write, in the notation (22.2),

$$(23.6)\qquad \begin{cases} \Psi(1,1;\tau;3,s) \\ = \pi^2 \sum [N(\mu^*)]^{\frac{1}{2}} \exp \pi i u(a - b + \tfrac{1}{2}) \cdot \exp \pi i b v \cdot P^*(\mu^*), \end{cases}$$

with the restriction

$$(23.7)\qquad \mu^* = a + b2^{\frac{1}{2}} + \tfrac{1}{2} \gg 0.$$

When $D = 12$, we write in the notation (22.3)

$$(23.8)\qquad \begin{cases} \Psi(1,1;\tau;3,s) \\ = (2\pi^2/3) \sum [N(\mu^*)]^{\frac{1}{2}} \exp \pi i u(a+b)/3^{\frac{1}{2}} \cdot \exp \pi i(b + \tfrac{1}{2})v \cdot P^*(\mu^*) \end{cases}$$

with the restriction

$$\mu^* = (a+b) + (b+\tfrac{1}{2})3^{\frac{1}{2}} >> 0. \tag{23.9}$$

Now if we are interested in the behavior of $\Gamma(u,v)$ in u, (as $u \to i\infty$), we must arrange μ^* in order of increasing values of $a - b + \frac{1}{2}$ when $D = 8$ and $a + b$ when $D = 12$. Thus, for $D = 8$, the first few terms are

$$\mu^* = 1/2, 3/2 + 2^{\frac{1}{2}}; 3/2, 5/2 + 2^{\frac{1}{2}}, 7/2 + 2 \cdot 2^{\frac{1}{2}}, 9/2 + 3 \cdot 2^{\frac{1}{2}}; \cdots;$$

and

$$\begin{aligned} (1/\pi^2)\Psi(1,1;\tau;3,s) &= \tfrac{1}{2}\exp(\pi iu/2)\,[P^*(\tfrac{1}{2}) + \exp\pi iv \cdot P^*(\tfrac{3}{2} + 2^{\frac{1}{2}})] \\ &+ \exp(3\pi iu/2)\,[3/2P^*(3/2) + 17^{\frac{1}{2}}/2P^*(5/2 + 2^{\frac{1}{2}})\exp\pi iv \\ &+ 17^{\frac{1}{2}}/2P^*(7/2 + 2 \cdot 2^{\frac{1}{2}})\exp 2\pi iv + 3/2P^*(9/2 + 3 \cdot 2^{\frac{1}{2}})\exp 3\pi iv] \\ &+ \cdots. \end{aligned} \tag{23.10}$$

For $D = 12$, the first few terms are

$$\mu^* = 1 + 3^{\frac{1}{2}}/2, 1 - 3^{\frac{1}{2}}/2; 2 + 3^{\frac{1}{2}}/2, 2 - 3^{\frac{1}{2}}/2; \cdots;$$

and

$$\begin{aligned} &(3/2\pi^2)\Psi(1,1;\tau;3,s) \\ &= \tfrac{1}{2}\exp(\pi iu/3^{\frac{1}{2}})[P^*(1 + 3^{\frac{1}{2}}/2) + \exp(-\pi iv/2)P^*(1 - 3^{\frac{1}{2}}/2)] \\ &+ 13^{\frac{1}{2}}/2\exp(2\pi iu/3^{\frac{1}{2}})[P^*(2 + 3^{\frac{1}{2}}/2) + \exp(-\pi iv/2)P^*(2 - 3^{\frac{1}{2}}/2)] \\ &+ \cdots. \end{aligned} \tag{23.11}$$

We next observe that for $D = 8$,

$$P^*(\mu) = 0 \text{ if } a \equiv b \bmod 2. \tag{23.12}$$

This is true because of a symmetry in the formula (23.4). For instance, if α/β has the property (23.5), so does $\alpha/\beta + (1+\eta)$. Now when α/β is augmented by $1 + \eta$, $H^8{}_{1,1}(\alpha/\beta)e(-\mu^*\alpha/\beta)$ is multiplied by

$$i^3 e(-\mu^*[1+\eta]) = -e([a+b]\eta),$$

which equals -1 when $a \equiv b \bmod 2$. Thus all terms of type $\exp \pi i(4s-1)u/2$ vanish in (23.10), and, in particular, differentiating with respect to v (at $v = 0$), we find, condition (22.9) supplemented by the strong result

$$\Gamma_t(u) = O(\exp 3\pi iu/2) \text{ as } u \to i\infty, \tag{23.13}$$

if we start by letting $\Xi = \Psi(d,c;\tau;3,0)$ in equation (22.7).

Turning our attention to $D = 12$, we are less fortunate;

$$P^*(\mu^*) = 0, \text{ if } a \not\equiv b \bmod 2, \tag{23.14}$$

since $H^{s}{}_{1,1}(\alpha/\beta)e(-\mu^{*}\alpha/\beta)$ becomes multiplied by $+e([a+b]\eta)$ when α/β is augmented by $1+\eta$. Thus all terms of type $\exp 2t\pi iu/3^{\frac{1}{2}}$ vanish in (23.11). Thus (22.10) can be supplemented only by the comparatively weak rsult

$$\Gamma_t(u) = O(\exp \pi iu/3^{\frac{1}{2}}), \tag{23.15}$$

if we start with $\Xi = \Psi$ in equation (22.7).

24. Completion of the identity for $D = 8$. We first take the case $D = 8$ where the rational modular group has the famous Klein invariant $J(u)$. The factors $-i$ in system (22.9) serves to forecast the presence of radicals. To simplfy matters, we take fourth powers:

$$\Gamma_t^{4}(u+1) = \Gamma_t^{4}(u), \tag{24.1a}$$

$$\Gamma_t^{4}(-1/u) = \Gamma_t^{4}(u)u^{8t+12}, \tag{24.1b}$$

$$\Gamma_t^{4}(u) = O[J^{-3}(u)] \text{ as } u \to i\infty, \tag{24.1c}$$

the last expression coming from (23.13). Thus

$$\Gamma_t^{4}(u) = J'(u)^{4t+6} f[J(u)] J(u)^{-t_1}[J(u)-1]^{-t_2}, \tag{24.2}$$

where, in the notation of "integral part" $[\cdot\ \cdot\ \cdot]$,

$$t_1 = 4 + [8t/3], \qquad t_2 = 2t + 3, \tag{24.3}$$

and the degree of f is $\leqq t_1 + t_2 - 4t - 9$, by the usual method of Poincaré [2].

Beyond these considerations $\Gamma_t^{4}(u)$ must behave like a perfect fourth power near every finite complex value of u:

t	t_1	t_2	max degree f
0	4	3	-2
1	6	5	-2
2	9	7	-1
3	12	9	0

Thus the first instance is, at $t = 3$,

$$\Gamma_3^{4}(u) = \text{const.}\, J'(u)^{18} J(u)^{-12}[J(u)-1]^{-9}. \tag{24.4}$$

The right-hand member indeed is a perfect fourth power. This will not *necessarily* imply that $\Gamma_3(u)$ transforms with the factors required in (22.9). (This requires continuation.) We have nevertheless established that in the terminology of § 22, $j \geqq 3$ for $D = 8$. Thus Ψ/Θ^3 is free of singularities and finally by Theorem 4,

$$\Psi(d, c; \tau; 3, 0) = \Theta^3(d, c; \tau), \tag{24.5}$$

$$A_3(\mu) = Z(\mu). \tag{24.6}$$

We can justify anew the assertion that

$$\Gamma_3^*(u) = J'(u)^{9/2}[J(u) - 1]^{-9/4} J(u)^{-3} \tag{24.7}$$

must necessarily satisfy the properties (22.9). For instance, such a $\Gamma_3(u)$ exists because Θ has only a simple zero and starting with $\Xi = \Psi$ in (22.7) we must necessarily arrive at a $\Gamma_3 \not\equiv 0$.

Continuing along the lines of the earlier part [16], we turn our attention to dimensionalities: The *modular* forms $\Xi(d, c; \tau)$ *described by equations* (16.3)-(16.7) *with* $k = 3$, $s = 0$, *are of dimension one* if they are bounded at infinity. To see this, we note that even in the absence of the special information in § 23, we can conclude that $\Gamma_t(u) = O(J^{-1/4}(u))$, from equations (22.9). Yet we could conceivably have more forms $\Gamma_t^4(u)$, since the degree of $f[J(u)]$ can now be $t_1 + t_2 - 4t - 7$. We still insist $\Gamma_t(u)$ must be single-valued in u regardless of how it transforms under the modular group. We then find these additional forms for Γ_0^4, Γ_2^4, Γ_3^4 are the only possibilities:

$$J'(u)^6/J(u)^4[J(u) - 1]^3, \qquad J'(u)^{14}/J(u)^8[J(u) - 1]^7,$$
$$J'(u)^{18}/J(u)^{12}[J(u) - 1]^7.$$

Even though these are fourth powers, their fourth roots are of the form $[J(u) - 1]^{\frac{1}{2}}\Gamma_3^*(u)$ (Rat. Funct. of J', J). Thus since $[J(u) - 1]^{\frac{1}{2}}$ acquires a sign change when $u \rightarrow u + 1$, it follows that the only solution to system (22.9) is still (24.7).

25. Failure of the identity for $D = 12$. Here we consider the transformation (22.10) for which Hecke's invariant $I(u)$ is most natural (see § 10). It has the properties

$$\begin{cases} I(u + 3^{\frac{1}{2}}) = I(u), \\ I(-1/u) = I(u), \\ I(u) = \text{const} \cdot \exp - 2\pi i u/3^{\frac{1}{2}} + O(1), \text{ as } u \rightarrow i\infty, \\ I(u) = \text{const} \cdot (u - i)^2 + 1 + O(u - i)^3, \text{ as } u \rightarrow i, \\ I(u) = \text{const} \cdot (u - \exp 2\pi i/6)^6 + O(u - \exp 2\pi i/6)^7, \\ \qquad\qquad\qquad\qquad \text{as } u \rightarrow \exp 2\pi i/6. \end{cases} \tag{25.1}$$

We note

$$(25.2)\qquad \begin{cases} \Gamma_t^4(u+3^{\frac{1}{2}}) = \Gamma_t^4(u), \\ \Gamma_t^4(-1/u) = \Gamma_t^4(u)u^{8t+12}, \\ \Gamma_t^4(u) = O[I(u)^{-2}] \text{ as } u \to i\infty. \end{cases}$$

Then by the usual method

$$(25.3)\qquad \Gamma_t^4(u) = I'(u)^{4t+6}f[I(u)]I(u)^{-t_1}[I(u)-1]^{-t_2},$$

where

$$(25.4)\qquad t_1 = 5 + [10t/3], \qquad t_2 = 2t+3$$

and f is a polynomial of degree $\leqq t_1 + t_2 - 4t - 8$. We then obtain the values

t	t_1	t_2	max degree f
0	5	3	0
1	8	5	1
2	11	7	2
3	15	9	4

While there are now plenty of polynomials, more important, many are *fourth* powers in the u-plane. For $t = 0, 1, 2$ we have the following exact fourth powers:

$$(24.5)\qquad \Gamma_0^*(u)^4 = I'(u)^6 I(u)^{-5}[I(u)-1]^{-3},$$

$$(24.6)\qquad \Gamma_1^*(u)^4 = I'(u)^{10} I(u)^{-7}[I(u)-1]^{-5},$$

$$(24.7)\qquad \Gamma_2^*(u)^4 = I'(u)^{14} I(u)^{-11}[I(u)-1]^{-5},$$

$$(24.8)\qquad \Gamma_2^{**}(u)^4 = I'(u)^{14} I(u)^{-11}[I(u)-1]^{-7}.$$

We can verify that $\Gamma_0^*(u) \approx \text{const} + O(u-i)$ hence comparing behaviors at $u = i$, $\Gamma_0^*(u)$ does not satisfy the required sign condition, i. e., $\Gamma_0(-1/u) = +i\Gamma_0(u)u^3$. Moreover, Γ_1^* and $\Gamma_2^* \approx \text{const}(u-i)$, hence they satisfy conditions (22.10), but Γ_2^{**} must be excluded since $\Gamma_2^{**}(u+3^{\frac{1}{2}}) = +\Gamma_2^{**}(u)$ from its order at $i\infty$. *Thus the modular forms $\Xi(d, c; \tau)$ described by equations (16.3)-(16.7) with $k = 3$, $s = 0$ are a vector space of dimension two, or three* if they are bounded at infinity.

We know that $\Psi(d, c; \tau; 3, 0) \neq \Theta^3(d, c; \tau)$ because $Z(1) = 8 \neq A_3(1) = 6$, so the coefficients of $e(\tau)$ do not match when $d = c = 0$. The third independent solution of the Ξ system is not apparent, if it exists at all.

26. Rational results. If we take the coefficient in Ψ for $e(\pi^2\mu\tau)$, namely $Z(\pi^2\mu)$, there is a very simple relation with $Z(\mu)$ in the case where

$\pi \in \mathfrak{O}_2$ is an odd prime not dividing the square-free totally positive μ. Using formulae (20.3) and (20.4) we find

$$(26.1) \qquad P_\pi(\mu\pi^2) = \begin{cases} P_\pi(\mu)\,(1+2)/|N(\pi)|), & N(\pi) > 0, \\ P_\pi(\mu), & N(\pi) < 0. \end{cases}$$

This is the only factor of $P(\mu)$ in (17.12) that changes, and the value of $N(\mu)$ of course also changes when $\mu\pi^2$ replaces μ. Thus it is easy to see that for $D = 8, 12$,

$$(26.2) \qquad Z(\mu\pi^2) = \begin{cases} Z(\mu)\,|N(\pi)|, & N(\pi) > 0, \\ Z(\mu)\,[|N(\pi)| + 2], & N(\pi) < 0. \end{cases}$$

In the case where $D = 8$, $Z(\mu) = A_3(\mu)$ and (26.2) gives us a theorem on the comparative number of representations of μ and $\pi^2\mu$ by three squares. Such theorems would not be easy to prove directly.

For example, we might start with $A_3(1) = 6$ and a prime

$$(26.3) \qquad p = 8K \pm 1,$$

so that in $R(2^{\frac{1}{2}})$

$$(26.4) \qquad \pm p = \pi\pi'.$$

Then using some of the results of (19.4) and (26.2) we learn the equation, in $R(2^{\frac{1}{2}})$,

$$(26.5) \qquad \pi^2 = \xi_1^2 + \xi_2^2 + \xi_3^2$$

has $48K$ non-trivial solutions (the triviality $\pi^2 = \pi^2$ counting for six additional ones). If

$$(26.6) \qquad p \equiv \pm 3 \pmod 8,$$

so that p is prime in $R(2^{\frac{1}{2}})$, the equation

$$(26.7) \qquad p^2 = \xi_1^2 + \xi_2^2 + \xi_3^2$$

has $6(p^2 - 1)$ non-trivial solutions.

It would be irrelevant to our goal to attempt to categorize the ensuing wealth of non-analytic results.

In concluding, we might note that starting with hyperelliptic integrals and using Hermite's analysis, Humbert [19] discovered that $D = 5, 8$, and 12 all enjoy a favored role in theta-function theory, but he did not press the matter far enough to discover any number theoretic results of intrinsic interest.

UNIVERSITY OF ARIZONA.

REFERENCES.

[16] H. Cohn, "Decomposition into four integral squares in the fields of $2^{\frac{1}{2}}$ and $3^{\frac{1}{2}}$," *American Journal of Mathematics*, vol 82 (1960), pp. 301-321.

[16a] H. Hasse, "Allgemeine Theorie der Gaussschen Summen in algebraischen Zahlkörpern," *Abhandlungen der deutschen Akademie der Wissenschaften zu Berlin*, Math.-Nat. Klasse (1951), no. 1.

[17] E. Hecke, "Bestimmung der Klassenzahl einer neuen Reihe von algebraischen Zahlkörpern," *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, Mathematisch-physikalische Klasse (1921), pp. 1-23.

[18] ———, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig (1923), chapter 8.

[19] G. Humbert, "Sur les fonctions abéliennes singulierès d'invariants huit, douze, et cinq," *Journal de Mathématiques Pures et Appliqueés*, ser. VI, vol. 2 (1906), pp. 329-355.

[20] E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig (1927), pp. 167 ff.

[21] H. Maass, "Konstruktion ganzer Modulformen halbzahliger Dimension mit ϑ-Multiplikatoren in einer und zwei Variabeln," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität*, vol. 12 (1938), pp. 133-162.

[22] ———, "Konstruktion ganzer Modulformen halbzähliger Dimension mit ϑ-Multiplikatoren in zwei Variabeln," *Mathematische Zeitschrift*, vol. 43 (1938), pp. 709-738.

[23] L. J. Mordell, "Note on class relation formulae," *Messenger of Mathematics*, vol. 45 (1916), pp. 76-80.

POINTS MULTIPLES D'UNE APPLICATION ET PRODUIT CYCLIQUE REDUIT.*

par ANDRÉ HAEFLIGER.

Le but essentiel de cette note est de déterminer la classe de cohomologie universelle modulo p duale au cycle des points p-uples d'une application f d'une variété V dans une variété M, p étant premier et les points p-uples étant considérés comme des points du produit cyclique de V. Cette classe peut aussi s'interprèter comme une obstruction à trouver dans la classe d'homotopie de f une application sans point p-uple. Elle est en relation étroite avec la classe de plongement Φ_p de Wu (cf. [13]).

La méthode utilisée donne une détermination explicite de la cohomologie modulo p du p-produit cyclique réduit V^*_p d'une variété V. C'est dans la cohomologie de cet espace que se trouvent des obstructions au plongement de V dans une variété M (cf. [13] et [7]). Nous retrouvons les conditions données par Wu pour l'annulation des classes Φ_p lorsque M est l'espace euclidien.

Je tiens à remercier vivement le Prof. N. E. Steenrod qui m'a communiqué ses résultats avant leur publication.

1. Définitions.

Ce paragraphe rappelle essentiellement les notions introduites dans [5].

1.1. *Point p-uple de type π d'une application.* Soit f une application continue d'un espace V dans un espace M. Un point p-uple de f est une suite $x_1, \cdots, x_p$ de p points distincts de V tels que $f(x_1) = \cdots = f(x_p)$. Mais il est naturel d'identifier deux telles suites si l'une se déduit de l'autre par une permutation. Soit donc π un groupe de permutations de p objets; il agit sur le produit V^p par permutation des facteurs et, par restriction, sur le sous-espace $V^p{}_0$ formé des suites de p points distincts de V. Soit $V^0{}_\pi$ le quotient de $V^p{}_0$ par l'action de π: deux points $(x_1, \cdots, x_p)$ et $(x'_1, \cdots, x'_p)$ de $V^p{}_0$ définissent le même point $\{x_1, \cdots, x_p\}$ de $V^0{}_\pi$ si l'une des suites est obtenue à partir de l'autre par une permutation appartenant à π. Par définition, *un point p-uple de f de type π* est un point $\{x_1, \cdots, x_p\}$ de $V^0{}_\pi$ tel que $f(x_1) = \cdots = f(x_p)$.

---

* Received June 8, 1960.

1.2. *Classe universelle des points p-uples.* Supposons que M soit une variété de dimension m. Soit $E_\pi \to B_\pi$ un espace fibré universel de groupe structural π. Soit $M^p{}_\pi$ le fibré $E_\pi \times_\pi M^p$ associé à E_π de fibre M^p sur laquelle π agit par permutation des facteurs. La reunion des diagonales des fibres forme un sous-fibré trivial $M_\pi = B_\pi \times M$: le sous-fibré diagonal.

On peut définir la classe $\Delta^M{}_\pi$ duale à M_π dans $M^p{}_\pi$ de la manière suivante. Soit $E'_\pi \to B'_\pi$ un fibré universel de groupe π pour une grande dimension N et tel que E'_π et B'_π soient des variétés; alors le fibré $M'^p{}_\pi$ associé à E'_π de fibre M^p est une variété ainsi que le sous-fibré diagonal M'_π. Soit $\Delta'^M{}_\pi$ la classe duale à la classe d'homologie de $M'^p{}_\pi$ représentée par la sous-variété M'_π; c'est un élément de $H^{(p-1)m}(M'^p{}_\pi)$, les coefficients étant les entiers modulo 2 si M est non orientable ou un faisceau d'entiers tordus si M est orientée. Il existe une représentation définie à l'homotopie près de $M'^p{}_\pi$ dans $M^p{}_\pi$; elle induit un isomorphisme de $H^{(p-1)m}(M^p{}_\pi)$ sur $H^{(p-1)m}(M'^p{}_\pi)$ si N est assez grand. Par définition $\Delta^M{}_\pi$ sera l'élément de $H^{(p-1)m}(M^p{}_\pi)$ correspondant à $\Delta'^M{}_\pi$ par cet isomorphisme.

La classe $\Delta^M{}_\pi$ (ou plus simplement Δ_π) sera la *classe universelle des points p-uples de type* π pour les applications continues dans M. Cette terminologie est justifiée dans les paragraphes qui suivent.

1.3. *La classe* $O^f{}_\pi$. L'espace $V^p{}_0$ (cf. 1.1) est un revêtement de $V^0{}_\pi$ et peut être considéré comme un fibré principal de groupe structural π. Soit alors comme plus haut E le fibré associé à $V^p{}_0$ de fibre M^p et soit D le sous-fibré diagonal formé de la réunion des diagonales des fibres. Toute application continue f de V dans M définit une section $f^0{}_\pi$ de E et le point $x = \{x_1, \cdots, x_p\}$ de $V^0{}_\pi$ est un point p-uple de f si et seulement si $f^0{}_\pi(x)$ appartient à D.

Si V est un espace assez raisonnable (par exemple un polyèdre), il existe une représentation h de E dans l'universel $M^p{}_\pi$ unique à l'homotopie près.

Par définition la classe $O^f{}_\pi$ *est égale à* $f^{0*}{}_\pi h^*(\Delta^M{}_\pi)$. Il est clair que $O^f{}_\pi$ ne dépend que la classe d'homotopie de f.

PROPOSITION. *Si f est homotope à une application de V dans M sans point p-uple, alors* $O^f{}_\pi = 0$.

En effet, si f est une application sans point p-uple, alors $hf^0{}_\pi$ applique $V^0{}_\pi$ dans $M^p{}_\pi - M_\pi$; d'autre part l'image de $\Delta^M{}_\pi$ par l'homomorphisme induit par l'injection de $M^p{}_\pi - M_\pi$ dans $M^p{}_\pi$ est nulle, car $\Delta^M{}_\pi$ est représentée par une cochaine de support M_π.

La classe $O^f{}_\pi$ représente dans un certain sens une première obstruction à trouver dans la classe d'homotopie de f une application sans point p-uple (cf. [7], [13]).

1.4. *Interprétation de la classe O^f_π dans le cas différentiable.* Soit f une application différentiable d'une variété V dans une variété M présentant sous forme régulière les points p-uples, c'est à dire que pour tout point p-uple $(x_1,\cdots,x_p)$ de f les images par f des espaces tangents à V en $x_1,\cdots,x_p$ sont en position générale dans l'espace tangent à M en $y=f(x_1)=\cdots=f(x_p)$. Ceci équivaut à dire que $f^p\colon V^p\to M^p$ est transverse (cf. [11]) sur la diagonale de M^p en tout point de $V^p{}_0\subset V^p$, ou encore que la section $f^0{}_\pi$ du fibré E est transverse sur le sous-fibré diagonal D. Dans ces conditions, *les points p-uples de type π de f forment une sous-variété dans $V^0{}_\pi$ représentant une classe d'homologie duale à $O^f{}_\pi$.* Cela résulte immédiatement de la définition de $O^f{}_\pi$ car $h^*(\Delta^M{}_\pi)$ est la classe duale à D dans E.

On peut remarquer (cf. [5], I, 3) que l'on peut toujours approcher une application donnée par une application différentiable qui présente sous forme régulière les p-uples sur un ouvert de $V^0{}_\pi$ qui en est un rétract par déformation.

1.5. *Produit cyclique réduit $V^*{}_p$ et classes de plongement $\phi^f{}_p$.* Soit p un nombre premier. Suivant la terminologie de Wu [13], appelons *p-produit cyclique réduit de V* le quotient $V^*{}_p$ de $V^p - V$ (p-produit de V privé de sa diagonale V) par l'action du groupe π des permutations cycliques des facteurs. Comme p est premier, l'espace $V^p - V$ est un revêtement à p feuillets de $V^*{}_p$ et peut être aussi considéré comme un espace fibré principal de groupe structural π. On peut donc construire comme plus haut (1.2 et 1.3) le fibré associé (de base $V^*{}_p$) de fibre M^p et l'on a une représentation h de E dans l'universel $M^p{}_\pi$; toute application continue f de V dans M définit une section f_p de E.

Par définition la classe $\phi^f{}_p\in H^{(p-1)m}(V^*{}_p)$ est égale à $f^*{}_p h^*(\Delta^M{}_\pi)$.

On remarquera que $O^f{}_\pi$ est l'image de $\phi^f{}_p$ par l'homomorphisme induit par l'injection du sous-espace $V^0{}_\pi$ dans $V^*{}_p$. Naturellement pour $p=2$, $O^f{}_\pi=\phi^f{}_p$.

PROPOSITION. *Si f est homotope à un plongement de V dans M, alors $\phi^f{}_p=0$.*

La démonstration est la même que celle de la proposition précédente.

Les classes $\phi^f{}_p$ généralisent au signe près les classes de plongement $\phi^{(p-1)m}{}_p$ définies par Wu lorsque M est l'espace euclidien R^m (cf. [13], II).

On pourrait aussi définir, suivant Wu (cf. [13], II), les classes d'immersion $\psi^f{}_p$ en prenant l'image de $\phi^f{}_p$ dans la limite inductive des cohomologies des voisinages de la diagonale dans le p-produit cyclique réduit de V. Si f est homotope à une immersion (c. à d. une application localement biunivoque), alors $\psi^f{}_p = 0$.

2. Résultats de Steenrod. Dans tout ce qui suit, p est un nombre premier et π est le groupe des permutations cycliques de p objets; T est un générateur de π. Tous les groupes de cohomologie considérés sont à coefficients les entiers modulo p.

2.1. *L'anneau de cohomologie du classifiant* B_π pour le groupe π sera noté $H^*(\pi)$ (cf. [3], Chap. XII).

Pour $p = 2$, $H^*(\pi) = P(\mu)$, où $P(\mu)$ est l'anneau des polynomes sur Z_2 dans la variable $\mu \in H^1(\pi)$.

Pour $p > 2$, $H^*(\pi) = P(\mu) \otimes E(\nu)$, où $P(\mu)$ est l'anneau des polynomes sur Z_p dans la variable $\mu \in H^2(\pi)$ et $E(\nu)$ l'algèbre extérieure engendrée par un élément $\nu \in H^1(\pi)$.

La cohomologie de tout espace fibré $q\colon E \to B$ à groupe structural π est une $H^*(\pi)$-algèbre: soit h l'application (définie à une homotopie près) de B dans B_π qui définit la classe de E; si $x \in H^*(E)$ et $\alpha \in H^*(\pi)$, par définition $\alpha x = q^* h^*(\alpha) \cup x$.

2.2. *Calcul de* $H^*(M^p{}_\pi)$. Soit M un complexe fini et soit $M^p{}_\pi$ le fibré associé à E_π de fibre M^p sur laquelle π agit par permutations cycliques des facteurs (cf. 1.2).

THÉORÈME (Steenrod). *Il existe un isomorphisme naturel de* $H^*(\pi)$-*algèbre* $\phi\colon H^*(M^p{}_\pi) \to H^*(\pi, H^*(M)^p)$.

La projection naturelle de $H^*(\pi, H^*(M)^p) = \sum_{r \geqq 0} H^r(\pi, H^*(M)^p)$ *sur* $H^0(\pi, H^*(M)^p)$ *identifié au sous-groupe des éléments invariants de* $H^*(M)^p = H^*(M^p)$ *correspond à l'homomorphisme* $r^*\colon H^*(M^p{}_\pi) \to H^*(M^p)$ *induit par l'injection de la fibre* $M^p{}_\pi$.

Dans cet énoncé, $H^*(M)^p$ est consideré comme un π-module (c. à d. un module sur l'anneau $Z(\pi)$ de π), π agissant par permutation cyclique des facteurs du produit tensoriel $H^*(M)^p$ avec le changement de signe usuel (cf. [3]).

2.3. Avant d'esquisser la démonstration, explicitons la structure de $H^*(\pi, H^*(M)^p)$

Soit D le sous-groupe de $H^*(M)^p$ formé des combinaisons linéaires des éléments diagonaux $(x)^p = x \otimes x \otimes \cdots \otimes x$, où $x \in H^*(M)$; le groupe π laisse fixe les éléments de D. *Comme π-module, $H^*(M)^p$ est somme directe de D et d'un sous-module libre.* Soit en effet (a_i) une base de $H^*(M)$; les éléments $a_{i_1} \otimes \cdots \otimes a_{i_p}$ forment une base de $H^*(M)^p$. Les éléments $a_i \otimes \cdots \otimes a_i$ forment une base de D et les autres éléments de la base engendrent un sous-module π-libre que l'on peut écrire sous la forme $Z_p(\pi) \otimes S$, où S est l'espace vectoriel sur Z_p engendré par une π-base.

Ainsi $H^*(M)^p = D + Z_p(\pi) \otimes S$ et donc

$$H^*(\pi, H^*(M)^p) = H^*(\pi) \otimes D + N,$$

où N désigne l'image de $H^*(M)^p$ par l'opérateur norme $N: 1 + T + \cdots + T^{p-1}$ (cf. [3], Chap. XII).

Le $H^*(\pi)$-module $H^*(\pi, H^*(M)^p)$ est donc engendré par le sous-groupe $D + N$ des éléments de π-degré 0 (un élément de $H^r(\pi, H^*(M)^p)$ est de π-degré r); de plus $H^*(\pi)$ agit trivialement sur les normes N (cf. [3], Chap. XII).

La structure multiplicative est déterminée en remarquant que les éléments de π-degré 0 forment un sous-anneau isomorphe à celui des éléments invariants de $H^*(M)^p$ et que $H^*(\pi) \otimes D$ est une sous-algèbre produit extérieure des anneaux $H^*(\pi)$ et D. On remarquera enfin que l'application de $H^*(M)$ sur D faisant correspondre à un élément x sa p-ème puissance tensorielsle $(x)^p$ est un homomorphisme d'anneaux *modulo N*.

2.4. La démonstration du théorème est en gros la suivante (pour plus de détails, voir [9]).

Soit W le complexe des chaines de B (résolution acyclique libre du π-module Z) et soient $C_*(M)$ (resp. $C^*(M)$) le complexe des chaines (resp. des cochaines) à coefficients Z_p de M. Alors $H^*(M^p{}_\pi)$ est la cohomologie du complexe double $\operatorname{Hom}(W \otimes_\pi C^*(M)^p, Z_p)$ qui s'identifie canoniquement au complexe double $\operatorname{Hom}_\pi(W, C^*(M)^p)$. Comme les coefficients sont dans un corps, il existe une équivalence naturelle (à l'homotopie près) entre le complexe de chaines $C^*(M)$ et $H^*(M)$ considéré comme un complexe de chaines avec opérateur bord zéro; il en résulte également que les π-complexes de chaines $C^*(M)^p$ et $H^*(M)^p$ sont équivalents. Donc $\operatorname{Hom}_\pi(W, C^*(M)^p)$ est équivalent (comme π-complexe) au complexe simple $\operatorname{Hom}_\pi(W, H^*(M)^p)$ dont la cohomologie est par définition $H^*(\pi, H^*(M)^p)$. Il existe donc un isomorphisme naturel $\phi: H^*(M^p{}_\pi) \to H^*(\pi, H^*(M)^p)$ de $H^*(\pi)$-modules.

La deuxième partie de l'énoncé résulte immédiatement de la définition de ϕ. Ceci montre que la restriction de ϕ aux éléments de π-degré 0 est un homomorphisme multiplicatif; comme $H^*(M)^p$ est engendré comme $H^*(\pi)$-module par ses éléments de π-degré 0 (cf. 2.3), il en résulte que ϕ est aussi un isomorphisme d'anneaux.

2.5. *L'homomorphisme* $i^*: H^*(M^p{}_\pi) \to H^*(M_\pi)$. Soit M_π le sous-fibré diagonal de $M^p{}_\pi$ (cf. 1.2) ; il est isomorphe au produit $B_\pi \times M$.

Avec l'identification du Théorème 2.2 et l'identification de $H^*(M_\pi)$ avec $H^*(\pi) \otimes H^*(M)$, l'homomorphisme i^* induit par l'injection de M_π dans $M^p{}_\pi$ sera un homomorphisme de $H^*(\pi)$-algèbre:

$$i^*: H^*(\pi, H^*(M)^p) \to H^*(\pi) \otimes H^*(M).$$

Il suffira de connaître i^* sur le sous-groupe $D + N = H^0(\pi, H^*(M)^p)$ qui engendre $H^*(\pi, H^*(M)^p)$. Comme $H^*(\pi)$ agit trivialement sur N et que $H^*(\pi) \otimes H^*(M)$ est un $H^*(\pi)$-module libre, on a $i^*(N) = 0$. La valeur de i^* sur D est donnée par le

THÉORÈME (Steenrod). *Soit x un élément de $H^q(M)$ et $(x)^p = x \otimes \cdots \otimes x$. On a $p = 2$, $i^*(x)^p = \sum_0^q \mu^{q-i} Sq^i x$,*

$$p > 2,\ i^*(x)^p = \sigma \sum_{i=0}^{[q/2]} (-1)^i \mu^{h(q-2i)} \mathcal{P}^i x - \sigma \sum_{i>0}^{[q/2]} (-1)^i \mu^{h(q-2i)-1} \nu \beta \mathcal{P}^i x,$$

où les $\mathcal{P}^i$ (resp. les Sq^i) sont les p-èmes puissances cycliques r-duites (resp. les carrés) de Steenrod (cf. [8]); β est l'homomorphisme $H^k(M, Z_p) \to H^{k+1}(M, Z_p)$ de Bockstein; $h = (p-1)/2$ et $\sigma = (-1)^{q/2}$ ou $(-1)^{(q-1)/2} h!$ suivant que q est pair our impair.

Pour la démonstration, cf. [9]. On remarquera que i^* est injectif sur le sous-module $H^*(\pi) \otimes D$.

3. Détermination de la classe universelle des points p-uples.

3.1. Soit M une variété connexe de dimension n, compacte, avec un bord B. Nous supposerons M orientée si $p > 2$. Pour tout nombre premier p et tout entier j positif, WU a défini (cf. [12]) les classes $U^j{}_{(p)}$ appartenant à $H^{2j(p-1)}(M, Z_p)$ pour $p > 2$ ou à $H^j(M, Z_2)$ pour $p = 2$ par les relations:

$$\langle Sq^j \alpha, M \rangle = \langle U^j{}_{(2)} \cup \alpha, M \rangle, \qquad p = 2,$$

$$\langle \mathcal{P}^j \alpha, M \rangle = \langle U^j{}_{(p)} \cup \alpha, M \rangle, \qquad p > 2,$$

pour tout élément α appartenant à $H^*(M \operatorname{mod} B, Z_p)$; le symbole $\langle \gamma, M \rangle$

désigne la valeur (indice de Kronecker) de $\gamma \in H^r(M, Z_p)$ sur le générateur de $H_m(M \operatorname{mod} B, Z_p)$ défini par l'orientation de M. Remarquons que $< \gamma, M > = 0$ si $r \neq m$.

Pour rester dans le cadre de la théorie précédente, nous supposerons que M est un complexe.

3.2. THÉORÈME. *La classe Δ_π modulo p duale au sous-fibré diagonal M de M^p est*

$$\Delta_\pi = \sum_{j=0}^{\leqq m/2} \mu^{m-2j} (U^j{}_{(2)})^2 + \delta_2, \qquad p = 2,$$

$$\Delta_\pi = \lambda \sum_{j=0}^{\leqq m/2p} (-1)^j \mu^{h(m-2jp)} (U^j{}_{(p)})^p + \delta_p \qquad p > 2,$$

où δ_p est la classe duale dans M^p à la classe d'homologie représentée par la diagonale, $h = (p-1)/2$ et $\lambda = (-1)^{m/2}$ ou $(-1)^{(m-1)/2} h!$ suivant que m est pair ou impair.

Pour exprimer Δ_π, on a identifié $H^*(M^p{}_\pi)$ à

$$H^*(\pi, H^*(M)^p) = \sum_{k>0} H^k(\pi) \otimes D + (D + N)$$

(cf. 2.3).

3.3. DÉMONSTRATION. Prenons pour E_π le complexe standard qui a p cellules dans chaque dimension $i \geqq 0$: $e_i, Te_i, \cdots, T^{p-1}e_i$, l'operateur bord étant défini par $\partial e_{2n} = (1 + T + \cdots + T^{p-1}) e_{2n-1}$ et $\partial e_{2n+1} = (1 - T) e_{2n}$.

Remplaçons le fibré $E_\pi \to B_\pi$ par le fibré $E'_\pi \to B'_\pi$ obtenu en enlevant de E_π toutes les cellules de dimension plus grandes que $(p-1)N - 1$, où $N > m$. Nous obtenons ainsi une décomposition cellulaire de la sphère $S^{(p-1)N-1}$ et B'_π est un espace lenticulaire de la même dimension. Soit $M'^p{}_\pi$ la restriction du fibré $M^p{}_\pi$ à B'_π.

Le même raisonnement que dans 2.4 montre qu'il existe un isomorphisme naturel de $H^*(\pi)$-module ϕ' tel que le diagramme suivant soit commutatif:

$$\begin{tikzcd}
H^*(M'^p{}_\pi) \arrow[r, "\phi'"] & H^*(B'_\pi, H^*(M)^p) \\
H^*(M^p{}_\pi) \arrow[r, "\phi"] \arrow[u, "j^*"] & H^*(B_\pi, H^*(M)^p) \arrow[u, "j^*"]
\end{tikzcd}$$

où les homomorphismes verticaux j^* sont induits par l'inclusion de $M'^p{}_\pi$ dans $M^p{}_\pi$ et B'_π dans B_π resp.; j^* est bijectif pour $r < (p-1)N - 1$, injectif pour $r = (p-1)N - 1$ et zéro pour $r > (p-1)N - 1$, r désignant le π-degré (cf. 2.3). De plus ϕ' est aussi multiplicatif (tout au moins sur l'image de j^* puisque ϕ et j^* sont des homomorphismes d'anneaux).

Choisissons un générateur S de $H_{(p-1)N-1}(B'_\pi, Z_p)$ tel que $< \mu^{N-1}, S > = 1$ si $p = 2$ et $< \mu^{kN-1}\nu, S > = 1$ si $p > 2$; soit $M \in H_m(M \bmod B, Z_p)$ le générateur défini par l'orientation de M. Alors les éléments $S \otimes M$ et $S \otimes M^p$ sont des classes d'homologie qui définissent des orientations modulo p de M'_π et M'^p_π respectivement.

Soit Δ_π la classe duale à M'_π relativement à ces orientations. Pour tout $x \in H^{(p-1)N-1+m}(M'^p_\pi)$, on a

3.4. $$< i^*(x), S \otimes M > = < x \cup \Delta_\pi, S \otimes M^p >$$

car par définition $\Delta_\pi \cap (S \otimes M^p) = i_*(S \otimes M)$ et $< x \cup \Delta_\pi, S \otimes M^p > =$ $< x, \Delta_\pi \cap (S \otimes M^p) > = < x, i_*(S \otimes M) > = < i^*(x), S \otimes M >$ (cf. [10]).

La formule 3.4 permet de calculer Δ_π modulo les normes N en appliquant mécaniquement 2.3 et 2.5. Montrons-le dans le cas $p = 2$. Posons $\Delta_\pi = \sum \mu^{m-2j}(V^j)^2$ modulo N, où $V^j \in H^j(M)$. Soit $\alpha \in H^{m-i}(M \bmod B)$ et soit $x = \mu^{N-m+2i-1}(\alpha)^2$. D'après 2.5, on a $i^*(x) = \sum \mu^{N+i-j-1} Sq^j \alpha = \mu^{N-1} Sq^i \alpha$ pour raison de dimensions. De même, d'après 2.3,

$$x \cup \Delta_\pi = \sum \mu^{N+2i-2j-1}(V^j\alpha)^2 = \mu^{N-1}(V^j\alpha)^2.$$

Donc

$$< i^*(x), S \otimes M > = < Sq^i\alpha, M > \text{ et } < x \cup \Delta_\pi, S \otimes M^2 > = < V^i\alpha, M >$$

d'où $V^i = U^i_{(2)}$.

Un calcul analogue donne dans le cas $p > 2$

$$\Delta_\pi = \lambda \sum_{0 \leqq j \leqq m/2p} (-1)^j \mu^{h(m-2jp)} (U^j_{(p)})^p \text{ modulo } N.$$

Pour déterminer Δ_π, il suffit de connaître so composante de π-degré 0 (cf. 2.3). Remarquons pour cela que l'injection r de la fibre M^p dans M'^p_π est transverse sur la sous-variété M'_π et que $r^{-1}(M'_\pi)$ est la diagonale de M^p. Donc $r^*(\Delta_\pi)$ est la classe duale δ_p à la diagonale dans M^p (cf. [11]); comme r^* est injectif sur les éléments de π-degré 0 et les identifie aux éléments invariants de $H^*(M^p)$ (cf. 2.2 et 2.3), le théorème est démontré.

3.5. *Classes caractéristiques de WU.* Posons

$$W^i = \sum_j Sq^{i-j} U^j_{(2)}$$

et

$$Q^i_{(p)} = \sum_j \mathfrak{P}^{i-j} U^j_{(p)}, \qquad p > 2.$$

Les classes W^i sont les classes de Stiefel-Whitney de M et les classes $Q^i_{(p)} \in H^{2(p-1)i}(M, Z_p)$ (notées aussi Q^i) sont les classes caractéristiques de Wu. Si M est une variété différentiable, ces classes sont des polynomes dans les classes de Pontryagin de M réduites modulo p (cf. [6]).

Considérons la classes $i^*(\Delta_\pi)$ restriction de Δ_π à M_π; elle peut s'interprèter comme la classe duale à la self-intersection de la "sous-variété" M_π de M^p_π; dans le cas différentiable, $i^*(\Delta_\pi)$ est la classe d'Euler du fibré normal à M_π dans M^p_π (c'est à dire la réunion des fibrés normaux aux diagonales des fibres ou encore la limite du fibré normal à M'_π dans M'^p_π lorsque N tend vers l'infini).

3.6. COROLLAIRE.

$$i^*(\Delta_\pi) = \sum_i \mu^{m-i} W^i, \qquad p = 2$$

$$i^*(\Delta_\pi) = \lambda \sum_k (-1)^k \mu^{h(m-2k)} Q^k{}_{(p)} - \lambda \sum_k (-1)^k \mu^{h(m-2k)-1} \nu \beta Q^k{}_{(p)}, \qquad p > 2.$$

Ces expressions se calculent immédiatement en appliquant 2.5 et 3.2. Lorsque M est une variété différentiable, alors $\beta Q^k{}_{(p)} = 0$ car les Q^k sont la réduction modulo p de classes entières (polynomes dans les classes de Pontryagin) (cf. [11], p. 63).

Les classes $i^*(\Delta_\pi)$ s'interprètent aussi comme classes universelles d'immersion dans M (cf. 1.5, 5.4).

3.7. *Expression de* $\phi^f{}_p$. Remarquons tout d'abord que $V^p_\pi - V_\pi$ a le même type d'homotopie que le p-produit cyclique réduit V^*_p de V. En effet $V^p_\pi - V_\pi = E_\pi \times_\pi (V^p - V)$ est fibré sur V^*_p avec une fibre contractile E_π. La projection q de cette fibration induit un isomorphisme naturel de $H^*(V^*_p)$ sur $H^*(V^p_\pi - V_\pi)$; avec cette identification, $j^*: H^*(V^p_\pi) \to H^*(V^*_p)$ désignera l'homomorphisme induit par l'injection j de $V^p_\pi - V_\pi$ dans V^p_π.

Toute application continue f de V dans M induit une application continue $\phi^p_\pi = 1 \times_\pi f^p$ de $V^p_\pi = E_\pi \times_\pi V^p$ dans $M^p = E_\pi \times_\pi V^p$. Avec les identifications de 2.2, ϕ^{p*}_π n'est autre que l'homomorphisme de $H^*(\pi, H^*(M)^p)$ dans $H^*(\pi, H^*(V)^p)$ induit par l'homomorphisme $f^{*p}: H^*(M)^p \to H^*(V)^p$.

On vérifie aisément (notations de 1.5) que $hf_\pi q$ est homotope à $\phi^p_\pi j$. Donc $\phi^f{}_p = j^*[\phi^{p*}_\pi \Delta_\pi]$.

Pour $p = 2$, on aura par exemple

$$\phi^f{}_2 = j^*[\sum \mu^{m-i}(f^* U^i)^2 + f^{2*}(\delta_2)].$$

L'homomorphisme j^* sera explicité au paragraphe suivant dans le cas où V est une variété.

4. Cohomologie modulo p du p-produit cyclique réduit d'une variété.

4.1. *Suites exactes associées à une sous-variété.* Soit V une sous-variété fermée de codimension q d'une variété paracompacte M. Dans ce paragraphe l'homologie ou la cohomologie sont à coefficients entiers ou modulo 2 suivant que les variétés sont orientées ou non, et la famille des supports est celle de tous les fermés. En utilisant la cohomologie définie par A. Borel dans [1] (cf. aussi [2]), U étant un voisinage ouvert de V, on a la suite exacte suivante:

$$\cdots \to H_k(V) \to H_k(U) \to H_k(U - V) \to H_{k-1}(V) \to \cdots$$

où le premier homomorphisme est induit par l'injection i de V dans U et le second par la restriction à $U - V$ des chaines de U. Si U' est un voisinage ouvert de V contenu dans U, cette suite exacte s'envoie par restriction dans la suite exacte analogue pour U'. En posant d'une part $U = M$ et en passant d'autre part à la limite directe suivant l'ordonné filtrant des voisinages de V, on a le diagramme commutatif et exact suivant:

$$\begin{tikzcd}
{} \arrow[r] & H_k(V) \arrow[r] \arrow[d] & H_k(M) \arrow[r] \arrow[d] & H_k(M - V) \arrow[r] \arrow[d] & {} \\
{} \arrow[r] & H_k(V) \arrow[r] & \text{lim. dir. } H_k(U) \arrow[r] & \text{lim. dir. } H_k(U - V) \arrow[r] & {}
\end{tikzcd}$$

Passons à la cohomologie par dualité de Poincaré (cf. [2]). L'injection de V dans U induit un isomorphisme de lim. dir. $H^r(U)$ sur $H^r(V)$ (cf. [4]). Avec cette identification et en notant $H^r(M \setminus V)$ la limite directe de $H^r(U - V)$ lorsque U parcourt les voisinages ouverts de V dans M, on a

4.2. PROPOSITION. *Le diagramme suivant est commutatif.*

$$\begin{tikzcd}
{} \arrow[dr] & & H^r(M) \arrow[r, "j^*"] \arrow[d] & H^r(M - V) \arrow[dr] \arrow[d] & & {} \\
& H^{r-q}(V) \arrow[ur, "\phi"] \arrow[dr, "\phi_0"'] & & & H^{r-q+1}(V) \arrow[ur] \arrow[dr] & \\
{} \arrow[ur] & & H^r(V) \arrow[r, "j^*_0"] & H^r(M \setminus V) \arrow[ur] & & {}
\end{tikzcd}$$

Les lignes horizontales sont exactes, ϕ est l'homomorphisme de Gysin déterminé par l'injection i de V dans M, j^* est induit par l'injection de $M - V$ dans M. L'homomorphisme ϕ_0 est déterminé par le cup produit par la classe $i^*(V^*)$, où V^* est la classe duale à V dans M.

Il reste à vérifier ce dernier point. Comme lim. dir $H^*(U) = H^*(V)$, pour tout $\alpha \in H^*(V)$, il existe un voisinage ouvert U de V et un élément $\beta \in H^*(U)$ tel que $i^*_U(\beta) = \alpha$, où i_U est l'injection de V dans U; si ϕ_U désigne l'homomorphisme de Gysin déterminé par i_U, on a $\phi_0(\alpha) = i^*_U \phi_U(\alpha) = i^*_U \phi_U(i^*_U \beta) = i^*_U(\beta \cup V^*) = \alpha \cup i^*(V^*)$.

Remarquons que si V est une sous-variété différentiable de M, alors $H^*(M \setminus V)$ s'identifie à la cohomologie du bord (espace fibré en sphères) d'un voisinage tubulaire de V et la deuxième suite exacte n'est autre que la suite exacte de Gysin.

On peut complèter le diagramme ci-dessus par des suites exactes verticales en faisant intervenir le groupe $H^*(M \operatorname{mod} V)$.

4.3. *Application à la "sous-variété" M_π de M^p_π.* Comme dans 3.3, réalisons E_π (resp. B_π) par une sphère (resp. un espace lenticulaire) de grande dimension $(p-1)N-1$. Ecrivons les suites exactes de 4.2 associées à la sous-variété M'_π de M'^p_π et passons à la limite en faisant tendre N vers l'infini. Nous obtenons les suites exactes:

$$\begin{tikzcd}
{} \arrow[dr] & & H^r(M^p_\pi) \arrow[r, "j^*"] \arrow[dd, "i^*"] & H^r(M^p_\pi - M_\pi) \arrow[dd] \arrow[dr] & & {} \\
& H^{r-(p-1)m}(M_\pi) \arrow[ur, "\phi"] \arrow[dr, "\phi_0"'] & & & H^{r-(p-1)m+1}(M_\pi) \arrow[ur] \arrow[dr] & \\
{} \arrow[ur] & & H^r(M_\pi) \arrow[r, "j^*_0"] & H^r(M^p_\pi \setminus M_\pi) \arrow[ur] & & {}
\end{tikzcd}$$

Nous avons vu dans 3.7 que $M^p_\pi - M_\pi$ a même type d'homotopie que le p-produit cyclique réduit M^*_p de M. Le même raisonnement montre que $H^*(M^p_\pi \setminus M_\pi)$ est canoniquement isomorphe à $H^*((M^p/\pi) \setminus M)$, où M^p/π est le p-produit cyclique de M (quotient de M^p par l'action de π) et où M est identifié à la diagonale de M^p/π.

D'autre part ϕ_0 est donné par le cup produit par la classe $i^*(\Delta_\pi)$. Or le terme de π-degré maximum dans $i^*(\Delta_\pi)$ est μ^{mh} (cf. 3.6); il en résulte que si $a \in H^*(M_\pi)$ est $\neq 0$, alors $a \cup i^*(\Delta_\pi)$ est $\neq 0$, donc que ϕ_0 est injectif. En vertu de la commutativité du diagramme, *ϕ est aussi injectif.*

Désignons par r^* (resp. r^*_0) les homomorphismes induits sur la cohomologie par l'injection de la fibre M^p (resp. M) dans M^p_π (resp. M_π) par ψ l'homomorphisme de Gysin déterminé par l'injection de la diagonale M dans M^p.

4.4. Compte tenu de ce qui précède, on a le diagramme commutatif et exact horizontalement:

$$\begin{tikzcd}
 & & H^r(M^p) & & \\
0 \arrow[r] & H^{r-(p-1)m}(M) \arrow[ur, "\psi"] & & & \\
 & & H^r(M^p{}_\pi) \arrow[uu, "r^*"'] \arrow[r, "j^*"] \arrow[dd, "i^*"] & H^r(M^*{}_p) \arrow[dr] \arrow[dd] & \\
0 \arrow[r] & H^{r-(p-1)m}(B_\pi \times M) \arrow[uu, "r^*{}_0"'] \arrow[ur, "\phi"] \arrow[dr, "\phi_0"'] & & & 0 \\
 & & H^r(B_\pi \times M) \arrow[r, "j^*{}_0"] & H^r((M^p/\pi)\backslash M) \arrow[ur] &
\end{tikzcd}$$

4.5. THÉORÈME. *L'homomorphisme* $j^*: H^r(M^p{}_\pi) \rightarrow H^r(M^*{}_p)$ *est surjectif. L'image par* j^* *d'un élément* $\alpha \in H^*(M^p{}_\pi)$ *est nulle si et seulement si*

a) *il existe un élément* $\beta \in H^*(B_\pi \times M)$ *tel que* $i^*(\alpha) = \beta \cup i^*(\Delta_\pi)$ (β *est alors unique*) *et*

b) $\psi r^*{}_0(\beta) = r^*(\alpha)$.

Les conditions a) et b) sont évidemment nécessaires d'après la commutativité de 4.4 et le fait que ϕ_0 est donné par le cup produit par $i^*(\Delta_\pi)$.

Réciproquement, supposons qu'il existe β tel que $i^*(\alpha) = \beta \cup i^*(\Delta_\pi)$; en vertu de 4.4, $\phi(\beta) - \alpha$ appartient au noyau de i^*; or ce noyau est contenu dans le sous-groupe des éléments de π-degré 0 de $H^*(M^p{}_\pi) = H^*(\pi, H^*(M)^p)$ (cf. 2.5); comme r^* est injectif sur ce sous-groupe (cf. 2.2), la condition $r^*(\phi(\beta) - \alpha) = 0$, équivalente à b), entraine $\alpha = \phi(\beta)$, donc $j^*(\alpha) = 0$.

Ce théorème permet le calcul explicite de $H^*(M^*{}_p)$ compte tenu des identifications $H^*(M^p{}_\pi) = H^*(\pi, H^*(M)^p)$, $H^*(B_\pi \times M) = H^*(\pi) \otimes H^*(M)$, des expressions explicites de i^* (cf. 2.5), de r^* (2.2) et de $i^*(\Delta_\pi)$ (cf. 3.6).

Quant à ψ, il est déterminé par la formule $\psi(\gamma) = (\gamma \otimes 1 \cdots \otimes 1) \cup \delta_p$, où δ_p est la classe duale à la diagonale M dans M^p (on a identifié $H^*(M^p)$ à $H^*(M)^p$); en effet, si i_0 est l'injection de la diagonale M dans M^p, $\gamma = i^*{}_0(\psi \otimes 1 \cdots \otimes 1)$ et la formule résulte de le propriété multiplicative de ψ.

5. Conditions pour l'annulation des classes de plongement $\varphi^f{}_p$.

5.1. *Classes caractéristiques normales d'une application.* Soit f une application continue d'une variété V de dimension n dans une variété M de dimension m. Soient $W = \sum W^i$ (resp. $W' = \sum W'^i$) la classe totale de Stiefel-Whitney de V (resp. M) et $Q = \sum Q^i$ (resp. $Q' = \sum Q'^i$) la classe caractéristique (totale) modulo p de Wu de V (resp. M) (cf. 3.5).

La classe totale de Stiefel-Whitney normale de f est la classe $\bar{W}_f = \sum \bar{W}^i{}_f = \bar{W} \cup f^*(W')$, où $\bar{W}$ est défini par $\bar{W} \cup W = 1$.

La classe caractéristique modulo p de Wu normale de f est la classe $\bar{Q}_f = \sum \bar{Q}^i{}_f = \bar{Q} \cup f^*(Q')$, où $\bar{Q}$ est défini par $\bar{Q} \cup Q = 1$.

Désignons par δ_p (resp. δ'_p) la classe duale à la diagonale de V^p (resp. M^p).

5.2. THÉORÈME. *La condition* $\phi^f{}_p = 0$ *est équivalente aux conditions*

a) $\bar{W}^k{}_f = 0,\ k > m - n$ pour $p = 2$,

$\bar{Q}^k{}_f = 0,\ k > (m-n)/2$ pour $p > 2$

et

b) $(\bar{W}^{m-n}{}_f \otimes 1) \cup \delta_2 = f^{2*}(\delta'_2)$ pour $p = 2$,

$\sigma(\bar{Q}^{(m-n)/2}{}_f \otimes 1 \cdots \otimes 1) \cup \delta_p = f^{p*}(\delta'_p)$ pour $p > 2$

où $\sigma = 1$ *ou* $(-1)^{(p+1)/2}$ *suivant que m et n sont tous deux pairs ou impair.*

5.3. *Démonstration.* Reprenons les notations de 3.7, 4.4 et 4.5. La restriction de $\phi^p{}_\pi$ à V_π est une application ϕ_π de V_π dans M_π. On a vu (3.7) que $\phi^f{}_p = j^*\phi^{p*}{}_\pi\Delta^M{}_\pi$. D'après 4.5, $\phi^f{}_p = 0$ si et seulement si a)' il existe $\beta \in H^*(B_\pi \times V)$ tel que $i^*(\phi^{p*}{}_\pi\Delta^M{}_\pi) = \beta \cup i^*(\Delta^V{}_\pi)$ et si b)' $\psi r^*{}_0(\beta) = r^*(\phi^{p*}{}_\pi\Delta^M{}_\pi)$. Ces conditions a)' et b)' sont équivalentes respectivement aux conditions a) et b) de 5.2. Montrons le pour $p = 2$.

En effet, $i^*\phi^{p*}{}_\pi(\Delta^M{}_\pi) = \phi^*{}_\pi i^*(\Delta^M{}_\pi) = \sum \mu^{m-j} f^*(W'^j)$. La condition a)' s'exprime sous la forme

a)' $$\sum \mu^{m-j} f^*(W'^j) = \beta \cup \sum \mu^{n-i} W^i.$$

Multiplions les deux membres par $\sum \mu^{n-j}\bar{W}^j$. On obtient la condition $\sum \mu^{m+n-k}\bar{W}^k{}_f = \mu^{2n}\beta$ qui équivaut à $\bar{W}^k{}_f = 0$ pour $k > m - n$.

On voit aussi que $r^*{}_0(\beta) =$ composante de π-degré 0 de $\beta = \bar{W}^{m-n}{}_f$. Dans le cas $p > 2$, on a $r^*{}_0(\beta) = \sigma\bar{Q}_f{}^{(m-n)/2}$. La condition b)' est bien équivalente à b) d'après la fin de 4.5.

5.4. *Les classes d'immersion* $\psi^f{}_p$. Il suit de cette démonstration que $\psi^f{}_p = 0$ est équivalent aux conditions a) de 5.2. En effet $\psi^f{}_p = j^*{}_0\phi^*{}_\pi i^*(\Delta^M{}_\pi)$.

5.5. COROLLAIRE (Wu). *Si f est une application de V dans l'espace euclidien* R^m, *la condition* $\phi^f{}_p = 0$ *est équivalente à*

$\bar{W}^k = 0$ pour $k \geqq m - n$ dans le cas $p = 2$

$\bar{Q}^k = 0$ pour $k \geqq (m-n)/2$ dans le cas $p > 2$.

5.6. *Le cas différentiable.* On sait alors (cf. [6]) que la classe normale

$\bar{Q}^k{}_f$ de f modulo p est un polynome dans les classes de Pontryagin normales $\bar{p}^i{}_f \in H^{4i}(V)$ de f réduites modulo p. Plus précisément, si $\bar{p}^i{}_f$ est formellement la i-ème fonction symétrique élémentaire $\sigma_i(x^2{}_1, \cdots, x^2{}_n)$, alors $\bar{Q}^k{}_f$ est la k-ème fonction symétrique élémentaire $\sigma_k(x^{p-1}{}_1, \cdots, x^{p-1}{}_n)$. Un calcul immédiat montre que la condition $\bar{Q}^k{}_f = 0$ pour $k > (m-n)/2$ est équivalente à $(\bar{p}^k{}_f)^h = 0$ modulo p pour $k > (m-n)/2$ et qu'alors $\bar{Q}_f{}^{(m-n)/2} = (\bar{p}_f{}^{(m-n)/2})^h$ modulo p, où $h = (p-1)/2$.

INSTITUTE FOR ADVANCED STUDY.

BIBLIOGRAPHIE.

[1] A. Borel, "The Poincaré duality in generalized manifolds," *Michigan Mathematical Journal*, vol. 4 (1957), pp. 227-239.

[2] ——— et J. Moore, "Homology and duality in generalized manifolds," Exp. II du *Seminar on transformations groups*, Annals of Mathematics Studies No. 46, Princeton, 1960.

[3] H. Cartan et S. Eilenberg, *Homological algebra*, Princeton, 1956.

[4] R. Godement, *Topologie algébrique et théorie des faisceaux*, Actualités Scientifiques et Industrielles, Paris, 1958.

[5] A. Haefliger, "Sur les self-intersections des applications différentiables," *Bulletin de la Société Mathématique de France*, vol. 87 (1959), pp. 351-359.

[6] F. Hirzebruch, "On Steenrod's reduced powers, the index of inertia and the Todd genus," *Proceedings of the National Academy of Sciences, USA.*, vol. 39 (1953), pp. 951-956.

[7] A. Shapiro, "Obstructions to the imbedding of a complex in a euclidean space. I. The first obstruction," *Annals of Mathematics*, vol. 66 (1957), pp. 256-269.

[8] N. Steenrod, "Homology groups of symmetric group and reduced power operations," *Proceedings of the National Academy of Sciences, USA*, vol. 39 (1953), pp. 213-223.

[9] ———, "Existence and uniqueness of the cyclic reduced powers," to appear.

[10] R. Thom, "Espaces fibrés en sphères et carrés de Steenrod," *Annales Scientifiques de l'Ecole Normale Supérieure*, vol. 69 (1952), pp. 109-181.

[11] ———, "Quelques propriétés globales des variétés différentiables," *Commentarii Mathematici Helvetici*, vol. 28 (1954), pp. 17-86.

[12] W. T. Wu, "Classes caractéristiques et i-carrés d'une variété," *Comptes Rendus* (Paris), vol. 230 (1950), pp. 508-511.

[13] ———, "On the realization of complexes in euclidean spaces, I, II, III," *Scientia Sinica*, vol. VII, No. 3 (1958), pp. 251-297, No. 4 (1958), pp. 365-387, vol. VIII, No. 2 (1959), pp. 133-150.

FINITE GROUPS ADMITTING A FIXED-POINT-FREE AUTOMORPHISM OF ORDER 4.*

By DANIEL GORENSTEIN and I. N. HERSTEIN.

Recently, in a remarkable piece of work [4, 5] John Thompson has proved a result which implies as an immediate corollary the well-known Frobenius conjecture, namely that a finite group admitting a fixed-point-free automorphism (i. e., leaving only the identity element fixed) of prime order must be nilpotent. However, non-nilpotent groups are known which admit fixed-point-free automorphisms of composite order. In all these cases one notices that the groups in question are solvable. Although the sample is rather restricted, it is not too unnatural to ask whether the condition that a finite group admit such an automorphism is strong enough to force solvability of the group. This question is related to another problem, which seems equally difficult, which asks whether a finite group containing a cyclic subgroup which is its own normalizer must be composite.

In the present paper we shall prove that a group G possessing a fixed-point-free automorphism of order 4 is solvable. Although many of the ideas used carry over to the case in which ϕ has order pq, and especially $2q$, our key lemmas use the fact that ϕ has order 4 in a crucial way.

The proof depends upon a theorem of Philip Hall which asserts that a finite group G is solvable if for every factorization of $o(G)$ into relatively prime numbers m and n, G contains a subgroup of order m. We show (Lemma 7) that a group G which has a fixed-point-free automorphism of order 4 satisfies the conditions of Hall's theorem.

Once we know that G is solvable it is not difficult to prove that its commutator subgroup is nilpotent (Theorem 2). This fact was also observed by Thompson.

Graham Higman has shown [3] that there is a bound to the class of a p-group P which possesses an automorphism ϕ of prime order q without fixed-points. This does not carry over to automorphisms of composite order, for at the end of the paper we give an example due to Thompson of a family of p-groups of arbitrary high class each of which admits a fixed-point-free automorphism of order 4.

---

* Received July 8, 1960; Minor revision December 8, 1960.

1. We begin by recalling a few well-known elementary results concerning a finite group G which admits a fixed-point-free automorphism ϕ of order n and in particular when $n=4$. First of all, for any prime $p \mid o(G)$ there is a unique p-Sylow subgroup P of G which is invariant under ϕ. We shall call P the *canonical* p-Sylow subgroup of G (with respect to ϕ). Furthermore, for any x in G we have the relation $x\phi(x)\phi^2(x)\cdots\phi^{n-1}(x)=1$.

If $n=4$, each orbit under ϕ except for that consisting of the identity contains either 2 or 4 elements, hence G is necessarily of odd order. The set of elements of G left fixed by ϕ^2 is a ϕ-invariant subgroup of G, which we denote by F. If $F \neq 1$, the restriction of ϕ to F is an automorphism of F of order 2 without non-trivial fixed elements. This implies that F is Abelian and that $\phi(f)=f^{-1}$ for all f in F. Finally, we shall denote by I the set of all h in G for which $\phi^2(h)=h^{-1}$. It is worth observing that I need not be a subgroup of G.

Throughout the paper G will denote a finite group having a fixed-point-free automorphism ϕ of order 4, F will denote the subgroup left elementwise fixed by ϕ^2 and I the subset consisting of those elements of G which are mapped into their inverses by ϕ^2.

LEMMA 1. $G=FI=IF$.

Proof. If $z=x^{-1}\phi^2(x)$ for some x in G, then $\phi^2(z)=\phi^2(x^{-1})\phi^4(x)=\phi^2(x^{-1})x=z^{-1}$, whence $z \in I$. Furthermore, $x^{-1}\phi^2(x)=y^{-1}\phi^2(y)$ implies that $\phi^2(xy^{-1})=xy^{-1}$ and hence that $xy^{-1} \in F$. Thus I contains at least $[G:F]$ elements.

To complete the proof, it will clearly suffice to show that distinct elements of I lie in distinct right (or left) cosets of F. If $h_2=fh_1$, $h_1, h_2 \in I$, $f \in F$, it follows by applying ϕ^2 that $h_2^{-1}=fh_1^{-1}$. Combining this with the previous relation gives $h_1^{-1}fh_1=f^{-1}$. Since G is of odd order, this forces $f=1$ and hence $h_1=h_2$. Similarly, we show that $h_2=h_1f$ implies $h_1=h_2$.

LEMMA 2. *If f_1, f_2 in F are conjugate in G, then $f_1=f_2$.*

Proof. Suppose $xf_1x^{-1}=f_2$. Since F is Abelian, we may assume without loss, in view of Lemma 1, that $x \in I$. Applying ϕ^2 gives $x^{-1}f_1x=f_2$, whence x^2 centralizes f_1. Since G is of odd order, x centralizes f_1, and consequently $f_1=f_2$.

As an immediate corollary, we obtain

LEMMA 3. *Any subgroup of F is in the center of its normalizer.*

LEMMA 4. *If $h \in I$, h commutes with $\phi(h)$.*

Proof. This lemma follows at once from the relations $h\phi(h)\phi^2(h)\phi^3(h) = 1$ and $\phi^2(h) = h^{-1}$.

LEMMA 5. *For any $p \mid o(G)$, F normalizes the canonical p-Sylow subgroup P of G.*

Proof. If $F \cap P = 1$, ϕ^2 is an automorphism of P of order 2 without non-trivial fixed elements, whence $\phi^2(x) = x^{-1}$ for all $x \in P$. Thus $P \subset I$. Let $f \in F$ and consider $P' = fPf^{-1}$. If $y = fxf^{-1}$, with $x \in P$, $\phi^2(y) = fx^{-1}f^{-1} = y^{-1}$, which implies that $P' \subset I$.

Suppose $P' \neq P$; choose y in P' and not in P. The subgroup generated by y and its image under ϕ is ϕ-invariant and, since $y \in I$, it follows from the preceding lemma that this subgroup is a p-group. Let P_1 be a maximal ϕ-invariant p-group containing y. If P_1 were not a p-Sylow subgroup of G, the unique ϕ-invariant p-Sylow subgroup P_2 of $N_G(P_1)$ would have order greater than $o(P_1)$ and would contain P_1 and consequently y. Since this would contradict our choice of P_1, P_1 must be a p-Sylow subgroup of G. Since P is the only ϕ-invariant p-Sylow subgroup of G, $P_1 = P$, which is impossible since $y \in P_1$, $y \notin P$. We conclude that $P' = fPf^{-1} = P$. Since f was arbitrary, $F \subset N_G(P)$.

Suppose, on the other hand, that $F \cap P \neq 1$. In this case we shall prove the lemma by induction on $o(G)$. Since F is Abelian, $F \cap P$ is a ϕ-invariant p-group which is normalized by F. If P_1 is a maximal ϕ-invariant p-group which is normalized by F, it follows first of all as in the preceding paragraph that $P_1 \subset P$. Suppose $P_1 < P$. We must have $N_G(P_1) = G$, for otherwise by induction F normalizes the unique ϕ-invariant p-Sylow subgroup P_2 of $N_G(P_1)$ and $o(P_2) > o(P_1)$. Thus $P_1 \lhd G$. Set $\bar{G} = G/P_1$ and let $\bar{\phi}$ be the image of ϕ on $\bar{G}$. $\bar{\phi}$ has no non-trivial fixed elements and is of order 2 or 4. If $\bar{P}$, $\bar{F}$ denote the images of P, F in $\bar{G}$, it follows by induction (or from the fact that $\bar{G}$ is Abelian in the case $\bar{\phi}^2 = 1$) that $\bar{F} \subset N_{\bar{G}}(\bar{P})$. Thus $F \subset N_G(P)$.

LEMMA 6. *If A, B are two ϕ-invariant subgroups of G which are each normalized by F, then ABF is a ϕ-invariant subgroup of G of order dividing $o(A)o(B)o(F)$.*

Proof. Since BF is a subgroup, ABF will be a subgroup if $(BF)A = A(BF)$. Since F normalizes A, it will suffice to show that $BA \subset ABF$.

Since A is ϕ-invariant, it follows from Lemma 1 applied to A that for any a in A, $a = a'f_1$, where $a' \in I \cap A$ and $f_1 \in F \cap A$. Similarly, for any b

in B, $b = f_2 b'$, $f_2 \in F \cap B$ and $b' \in I \cap B$. Clearly, $ba = f_2 b' a' f_1 \in ABF$ if and only if $b'a' \in ABF$.

Now $b'^{-1} a'^{-1} = fh$ for some f in F, h in I; applying ϕ^2 gives $b'a' = fh^{-1}$. Since $h^{-1} = a'b'f$ from the first relation, $b'a' = fa'b'f = a''b''f^2$, where $a'' \in A$, $b'' \in B$. Thus ABF is a subgroup as asserted. The remaining parts of the lemma are immediate.

LEMMA 7. *Let $p_1, p_2, \cdots, p_k$ be a set of primes dividing $o(G)$ and let $P_1, P_2, \cdots, P_k$ be the corresponding canonical Sylow subgroups of G. Then $P_1 P_2 \cdots P_k$ is a subgroup of G.*

Proof. By induction on k we may assume that $H = P_1 P_2 \cdots P_{k-1}$ is a subgroup of G. Clearly H is ϕ-invariant. By Lemma 5 $F \subset N_G(H)$ and $F \subset N_G(P_k)$, so that $S = HP_kF$ is a ϕ-invariant subgroup of G by Lemma 6. Since $o(S) \mid o(H) o(P_k) o(F)$, a q-Sylow subgroup Q of F for any prime $q \neq p_i$, $i = 1, 2, \cdots, k$, is a q-Sylow subgroup of S. By Lemma 3 Q is in the center of its normalizer in S, so that by a well-known theorem of Burnside S possesses a normal q-complement L_q. Since L_q consists of the elements of S of order prime to q, L_q contains H and P_k. Repeating this argument for each such prime $q \mid o(F)$, we readily conclude that $\bigcap_{\substack{q \mid o(F) \\ q \neq p_i}} L_q = HP_k = P_1 P_2 \cdots P_k$, which, being an intersection of subgroups, is a subgroup.

Lemma 7 leads at once to our main result.

THEOREM 1. *If G is a finite group admitting an automorphism of order 4 leaving only the identity element of G fixed, then G is solvable.*

Proof. It follows from Lemma 7 that for any factorization of $o(G)$ into the product of relatively prime numbers m and n, G contains a subgroup of order m. By a theorem of Philip Hall ([2], Theorem 9. 3. 3, p. 144), this implies that G is solvable.

2. We shall now examine the structure of G more closely, For our main result we need several lemmas.

LEMMA 8. *If $G = HM$, where H is nilpotent, normal in G, $(o(H), o(M)) = 1$, M is invariant under ϕ and $M \cap F = 1$, then $G = H \times M$.*

Proof. Let $\Phi(H)$ be the Frattini subgroup of H and set $\bar{G} = G/\Phi(H) = \bar{H}\bar{M}$. Since $(o(H), o(M)) = 1$, it follows from the properties of the Frattini subgroup that $\bar{G} = \bar{H} \times \bar{M}$ implies $G = H \times M$. Hence, without loss, we may assume that H is elementary Abelian. Since ϕ^2 leaves only the identity element of M fixed, M is Abelian. If either H contains two disjoint ϕ-invariant subgroups normal in G or ϕ does not act irreducibly on M, the lemma follows easily by induction. Hence we may assume that ϕ acts irreducibly on M and no proper ϕ-invariant subgroup of H is normal in G. In particular, this implies that H is an elementary Abelian p-group for some prime p.

The holomorph of ϕ and M is represented irreducibly on H regarded as a vector space over the prime field K_p with p elements. Let H^* be the corresponding vector space over the algebraic closure K^*_p of K_p. If M does not centralize H, it follows from Lemma 3.1 of [1] that with respect to a suitable basis of H^* the matrix of ϕ assumes the form

$$\begin{bmatrix} \phi_1 & & & & 0 \\ & \phi_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ 0 & & & & \phi_s \end{bmatrix},$$

where

$$\phi_i = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ b_i & 0 & 0 & 0 \end{bmatrix}$$

with $b_i \in K^*_p$. Since $\phi^4 = 1$, $\phi_i^4 = 1$ and hence $b_i = 1$ for all i. But this means that 1 is a characteristic root of ϕ and hence that ϕ leaves some element of H other than the identity fixed. This contradiction forces M to centralize H, and consequently $G = H \times M$, as asserted.

LEMMA 9. *If $G = HM$, where H is nilpotent, normal in G, $(o(H), o(M)) = 1$, M is invariant under ϕ and $C_G(H) \subset H$, then $M \subset F$.*

Proof. By Theorem 1 G and hence M is solvable. Let K be a maximal ϕ-invariant normal subgroup of M. By induction applied to HK, $K \subset F$. Let $\bar{M} = M/K$ and let $\bar{\phi}$ be the image of ϕ on $\bar{M}$. If $\bar{\phi}^2 = 1$ on $\bar{M}$, it follows readily that $M \subset F$. Hence we may assume that $\bar{\phi}$ has order 4 on $\bar{M}$. Since $\bar{M}$ is elementary Abelian and $\bar{\phi}$ acts irreducibly on $\bar{M}$, $\bar{\phi}^2(\bar{y}) = \bar{y}^{-1}$ for all $\bar{y}$ in $\bar{M}$. Thus for all y in M, $\phi^2(y) = y^{-1}z$, $z \in K$. Now if $x \in K$, $yxy^{-1} = x'$ for some $x' \in K$. Applying ϕ^2 gives $y^{-1}zxz^{-1}y = x'$. Since K is abelian we easily conclude that y^2 and consequently y centralizes x. Hence K is in the center of M.

As in the previous lemma we may assume without loss of generality that

H is elementary Abelian. By Lemma 1 applied to M, $M = (F \cap M)(I \cap M)$, and under our present assumptions $I \cap M \neq 1$. By induction we may suppose that no ϕ-invariant proper subgroup of H is normal in H; and we shall then derive a contradiction by showing that $I \cap M$ centralizes H.

Now $C_G(K)$ is ϕ-invariant and contains M, since K is in the center of M. Since $H_1 = H \cap C_G(K) \lhd C_G(K), N_G(H_1)$ contains M and H, whence $H_1 \lhd G$. Since H_1 is invariant under ϕ, the minimality of H implies that either $H_1 = 1$ or $H_1 = H$.

Suppose first that $H_1 = 1$. Since $K \subset F$ and F is Abelian $H \cap F \subset C_G(K)$, whence $H \cap F = 1$ and consequently $H \subset I$. If $y \in M \cap I$, $x \in H$, $yxy^{-1} = x'$ for some x' in H. Applying ϕ^2, we obtain $y^{-1}x^{-1}y = x'^{-1}$, which together with the preceding relation implies that x and y commute. Thus $I \cap M \subset C_G(H)$ as asserted.

On the other hand, if $H_1 = H$, K centralizes H, whence $K = 1$ and $I \cap M = M$. Since $M \cap F = 1$, $G = H \times M$ by Lemma 8. Thus $I \cap M$ centralizes H, completing the proof.

Lemma 10. *G has p-length* 1 *for all* $p \mid o(G)$.

Proof. Since G is solvable by Theorem 1, the statement of the lemma is meaningful. The proof will be by induction on $o(G)$. Let M be the maximal normal subgroup of G of order prime to p, and assume first that $M \neq 1$. M is ϕ-invariant since it is characteristic in G. Let $\bar{\phi}$ be the image of ϕ on $\bar{G} = G/M$. If $\bar{\phi}^2 = 1$ on $\bar{G}$, $\bar{G}$ is Abelian. If $\bar{\phi}$ has order 4 on $\bar{G}$, it follows by induction that $\bar{G}$ has p-length 1 and hence that a p-Sylow subgroup $\bar{P}$ of $\bar{G}$ is normal in $\bar{G}$. In either case we conclude that G has p-length 1. We may therefore suppose that $M = 1$.

Let P_1 be the maximal normal p-group of G and consequently ϕ-invariant. Let P be the canonical p-Sylow subgroup of G and $\tilde{P}$ its image in $\tilde{G} = G/P_1$. If $\tilde{K}$ is the maximal normal subgroup of $\tilde{G}$ of order prime to p, it follows by induction that the image of $\tilde{P}$ in $\tilde{G}/\tilde{K}$ is normal in $\tilde{G}/\tilde{K}$ whence $\tilde{P}\tilde{K} \lhd \tilde{G}$. If $\tilde{P}\tilde{K} < \tilde{G}$, its inverse image $G_0 < G$, and hence by induction has p-length 1.

Since P_1 contains its own centralizer in G ([2], Theorem 18.4.4, p. 332), G_0 contains no non-trivial normal subgroups of order prime to p and hence $P \lhd G_0$. But then $\tilde{P} \lhd \tilde{P}\tilde{K}$, and since $\tilde{P}$ is characteristic in $\tilde{P}\tilde{K}$, we conclude that $\tilde{P} \lhd \tilde{G}$, whence $P \lhd G$.

We may therefore assume that $\tilde{G} = \tilde{P}\tilde{K}$. The inverse image G_1 of $\tilde{K}$ is of the form P_1K, where K has order prime to p. Since G_1 is solvable, any two subgroups of G_1 of order $o(K)$ are conjugate ([2], Theorem 9.3.1, p. 141). One can now show by the same argument which proves the existence of canonical p-Sylow subgroups that there exists a unique conjugate of K in G, which is invariant under ϕ. Without loss we may assume K itself is ϕ-invariant. Since $C_{G_1}(P_1) \subset P_1$, the previous lemma implies that $K \subset F$. But then by the argument of the first paragraph of the lemma $\bar{K}$ is in the center of $\bar{G}$, whence $\bar{P} \lhd \bar{G}$ and $P \lhd G$.

THEOREM 2. *If G possesses an automorphism ϕ of order 4 leaving only the identity element fixed, then the commutator subgroup of G is nilpotent.*

Proof. G is solvable by Theorem 1. Assume first that G contains two minimal ϕ-invariant normal subgroups N_1 and N_2. Since the image of ϕ on G/N_1 and G/N_2 has no non-trivial fixed elements, the commutator subgroups $[G/N_i, G/N_i]$ of G/N_i, $i = 1, 2$, are nilpotent by induction. Let H_i be the inverse image of $[G/N_i, G/N_i]$ in G and set $H = H_1 \cap H_2$. Clearly, $H \lhd G$ and $[G, G] \subset H$. Furthermore, if x and y are elements of relatively prime order in H, their images in G/N_i, $i = 1, 2$, commute, and hence $y^{-1}xyx^{-1} \in N_1 \cap N_2$. Since N_1 and N_2 are distinct minimal normal ϕ-invariant subgroups of G, $N_1 \cap N_2 = 1$, and consequently x, y commute. Thus H and hence $[G, G]$ is nilpotent.

We may therefore suppose that G contains a unique minimal normal ϕ-invariant subgroup N_1. N_1 is a p-group for some prime p and G contains no non-trivial normal subgroups of order prime to p. Since G has p-length 1 by Lemma 10, a p-Sylow subgroup P of G is normal in G. Now $C_G(P) \lhd G$ and $C_G(P) = Z(P) \times K$, where K has order prime to p. Since K is characteristic in $C_G(P)$, K is normal in G, whence $K = 1$ and $C_G(P) \subset P$. Furthermore, $G = PM$ for some subgroup M of G, and we may assume M is invariant under ϕ. Since $(o(P), o(M)) = 1$, we can apply Lemma 9 to conclude that $M \subset F$. Thus M is Abelian, and consequently $[G, G] \subset P$ is nilpotent.

3. We conclude with an example of a family of p-groups of arbitrarily high class each of which has a fixed-point free automorphism of order 4. Let p be any prime such that $p \equiv 1 \pmod 4$ and let P_1 be an elementary Abelian p-group of order p^t, where $t = p^d$, d an arbitrary integer, and let $x_1, x_2, \cdots, x_t$ be a basis for P_1. We construct an extension of P_1 by adjoining a new letter y satisfying the relations:

$$(*) \qquad y^t = 1, \quad yx_iy^{-1} = x_ix_{i+1}, \quad i = 1, 2, \cdots, t-1, \quad yx_ty^{-1} = x_t.$$

These relations define a p-group of order tp^t and of class t.

Since $p \equiv 1 \pmod 4$, there is an integer α such that $\alpha^2 \equiv -1 \pmod p$.

We define an automorphism θ of P by setting $\theta(y)=y^{-1}$, $\theta(x_t)=x_t^{\alpha}$. For θ to be an automorphism, its value on x_i must be such that

$$(**) \qquad y^{-1}\theta(x_i)y=\theta(x_i)\theta(x_{i+1}).$$

Assume θ has been defined on x_j for $j>i$ and that $\theta(x_j)$ is in the subgroup generated by $x_j, x_{j+1},\cdots,x_t$. We shall show that $\theta(x_i)$ can be defined satisfying (**) and subject to the restriction $\theta(x_i)=x_i^{a_i}x_{i+1}^{a_{i+1}}\cdots x_t^{a_t}$. It follows at once from (**) that we have $x_{i+1}^{-a_i}x_{i+2}^{-a_{i+1}}\cdots x_t^{-a_{t-1}}=y\theta(x_{i+1})y^{-1}$. Since these relations have a solution for $a_i, a_{i+1},\cdots,a_{t-1}$ (for any choice of a_t), the automorphism θ exists.

Regarding P_1 as a vector space, it is easy to see that the matrix of θ with respect to the basis $x_1, x_2,\cdots,x_t$ has the form $\alpha D+N$, where $D=\operatorname{diag}(1,-1,1,-1,\cdots,1)$ and N is a strictly triangular matrix. It follows that the order of θ on P_1 is $4p^s$ for some $s\leqq d$. Setting $\phi=\theta^{p^s}$, ϕ has order 4 on P_1 and since $\phi(y)=y^{-1}$, ϕ has order 4 on P. The characteristic roots of ϕ are $\pm\alpha$, the same as those of θ. Since $\alpha\neq\pm 1$, ϕ leaves only the identity element of P_1 fixed. Since $\phi(y)=y^{-1}$, this implies that ϕ leaves only the indentity element of P fixed.

CLARK UNIVERSITY,
CORNELL UNIVERSITY.

REFERENCES.

[1] Daniel Gorenstein, "Finite groups which admit an automorphism with few orbits," *Canadian Journal of Mathematics*, vol. 12 (1960), pp. 73-100.

[2] Marshall Hall, *The Theory of Groups*, New York, 1959.

[3] Graham Higman, "Groups and rings having automorphisms without trivial fixed elements," *Journal of the London Mathematical Society*, vol. 32 (1957), pp. 321-334.

[4] John G. Thompson, "Finite groups with fixed-point-free automorphisms of prime order," *Proceedings of the National Academy of Sciences*, vol. 45 (1959), pp. 578-581.

[5] ———, "Normal p-complements for finite groups," *Mathematische Zeitschrift*, vol. 72 (1960), pp. 332-354.

ON INDUCED REPRESENTATIONS.*

By Robert J. Blattner.

1. Introduction. The purpose of this paper is threefold: to lay the foundations of a theory of induced representations of (not necessarily separable) locally compact groups, to prove a sharpened form of an intertwining number theorem due to Bruhat, and to prove a disjointness theorem for representations of Lie groups induced from compact subgroups. G. W. Mackey in [10] developed a notion of induced representation when the group G induced up to is separable and the inducing representation L is in a separable Hilbert space $\mathfrak{V}$. Because the construction rested on the choice of a quasi-invariant measure in the relevant homogeneous space and because the existence of such measures is problematical when G is not separable, this definition is not suitable for generalization to the non-separable case. The definition we employ, which is equivalent to Mackey's when G and $\mathfrak{V}$ are separable, is a modification of the one used by F. Bruhat in [3]. The chief novelty is the way in which the Hilbert space structure is defined on the function space $\mathfrak{H}$ in which the induced representation U^L operates, a way which owes much to Mackey's notion of intrinsic Hilbert space. Section 2 deals with the basic properties of induced representations, concluding with the theorem on induction in stages (Theorem 1).

In Sections 3 through 5 we are concerned with the problem, already considered by Bruhat, of finding the intertwining number of two inductions when G is a Lie group. Our method is based on two facts: (1) any function f in $\mathfrak{H}$ which is in the domain $\mathfrak{H}_\infty$ of all the operators of the differential representation ∂U^L of the enveloping algebra $\mathfrak{E}$ of the Lie algebra of G is essentially continuous; (2) if $X \in \mathfrak{E}$ is elliptic as a left invariant differential operator on G and has sufficiently high order, then $f(e)$ may be estimated in terms of $\partial U^L(X)f$ when $f \in \mathfrak{H}_\infty$. Our estimate of the intertwining number (Theorem 3) is in terms of the dimension of a certain space of distributions, the order of which is usually much lower than that needed in Bruhat's theorem. This would seem to result from our use of *unitary* representations throughout our discussion and our replacement of Schwartz's kernel theorem by the facts on elliptic operators mentioned above. The importance in other connections

---

* Received July 19, 1960.

of the theory of elliptic operators for Lie group representation theory has been established in recent papers by Stinespring ([15]) and Nelson and Stinespring ([12]). In Section 6 we prove a disjointness criterion for inductions to Lie groups of finite dimensional representations of compact subgroups (Theorem 4). This is accomplished by applying direct integral techniques to the results of Section 5. The paper concludes with an example in Section 7.

Notation. If f is a numerical function on a set S, $\| f \|_S = \mathrm{LUB}[|f(s)| : s \in S]$. If O is an open subset of a topological space and if $\mathcal{X}$ is a topological linear space, $C(O;\mathcal{X})$ denotes the class of all continuous functions from O to $\mathcal{X}$ and $C_0(O;\mathcal{X})$ denotes the subclass of $C(O;\mathcal{X})$ consisting of functions with compact support. A superscript ∞ (resp. $+$) indicates restriction to indefinitely differentiable (resp. non-negative) functions. If $\mathcal{Y}$ is another topological linear space, $\mathcal{L}(\mathcal{X};\mathcal{Y})$ is the space of all continuous linear maps of $\mathcal{X}$ into $\mathcal{Y}$ equipped with the topology of bounded convergence.

The author wishes to acknowledge his indebtedness to R. S. Phillips for several conversations on partial differential operators.

2. Induced representations. Let G be a locally compact group, Γ a closed subgroup of G, and L a unitary representation of Γ on the Hilbert space $\mathfrak{V}$. Let right Haar measure be chosen in G and Γ, and let their respective modular functions be Δ and δ. Let $\mathfrak{F}^*$ be the set of all functions f from G to $\mathfrak{V}$ such that: (1) $f(\cdot)$ is Bourbaki measurable (see [2], p. 180); (2) $f(\xi x) = \Delta(\xi)^{-\frac{1}{2}}\delta(\xi)^{\frac{1}{2}}L_\xi f(x)$ whenever $\xi \in \Gamma$ and $x \in G$; (3) $\| f(\cdot) \|^2$ is locally integrable. Let $M = G/\Gamma$ (right coset space) and let π be the canonical projection of G on M. As in Lemma 1.5 of [10], $\| f(\cdot) \|^2$ defines a positive Radon measure μ_f on M via the equation

$$\int_G \| f(x) \|^2 g(x)\,dx = \int_M (\tau g)(p)\,d\mu_f(p),$$

where $g \in C_0(G)$ and $(\tau g)(\pi(x)) = \int_\Gamma g(\xi x)\,d\xi$. Set $\| f \| = \mu_f(M)^{\frac{1}{2}}$ and $\mathfrak{F} = [f \in \mathfrak{F}^* : \| f \| < \infty]$. One easily sees that $\mathfrak{F}^*$ and $\mathfrak{F}$ are linear spaces.

If $f, g \in \mathfrak{F}$, then $(f(\cdot), g(\cdot))$ is Bourbaki measurable ([2], Proposition 10, p. 193) and $(f(\cdot), g(\cdot))$ defines a finite complex valued Radon measure on M, call it $\mu_{f,g}$, in the same way that $\| f(\cdot) \|^2$ defines μ_f. We set $(f, g) = \mu_{f,g}(M)$. $(\cdot,\cdot)$ is a positive semi-definite Hermitian form on F and $\| f \| = (f, f)^{\frac{1}{2}}$. Clearly $\| f \| = 0$ if and only if $f(\cdot) = 0$ locally almost everywhere (l. a. e.). Thus, if we set $\mathfrak{H} = \mathfrak{F}/[f \in \mathfrak{F} : f(\cdot) = 0 \text{ l. a. e.}]$, we may transport $(\cdot,\cdot)$ to $\mathcal{H}$ and $\mathcal{H}$ is then a pre-Hilbert space. (In the sequel, we shall often willfully confuse $\mathcal{F}$ and $\mathcal{H}$.)

In order to show completeness, we need the following estimate, which is also useful in other connections.

LEMMA 1. *For each compact subset K of G, there is a constant Λ_K such that, for all $f \in \mathcal{F}$,*

$$\int_K \| f(x) \| \, dx \leqq \Lambda_K \| f \|.$$

Proof. Choose $g \in C_0^+(G)$ such that $g = 1$ on K. Then

$$\int_K \| f(x) \|^2 \, dx \leqq \int_G g(x) \| f(x) \|^2 \, dx = \int_M (\tau g)(p) \, d\mu_f(p) \leqq \| f \|^2 \| \tau g \|_M.$$

Set $\Lambda_K = (\| \tau g \|_M \int_K dx)^{\frac{1}{2}}$ and apply the Schwarz inequality.

PROPOSITION 1. *$\mathcal{H}$ is complete.*

Proof (after Riesz-Fischer). Let $\{f_n\}$ be a Cauchy sequence in $\mathcal{F}$. As usual it suffices to show $\{f_n\}$ has a limit in $\mathcal{F}$ under the added assumption that $\| f_n - f_{n+1} \| < 2^{-n}$. First we show that for locally almost all $x \in G$, $\operatorname*{Lim}_{n \to \infty} f_n(x)$ exist in $\mathcal{V}$. In fact, let K be a compact subset of G. Lemma 1 tells us that $\int_K \| f_n(x) - f_{n+1}(x) \| \, dx < 2^{-n} \Lambda_K$, whence

$$\int_K \Big(\sum_1^\infty \| f_n(x) - f_{n+1}(x) \| \Big) dx < \Lambda_K.$$

Therefore for locally almost all $x \in K$, $\{f_n(x)\}$ is Cauchy in $\mathcal{V}$. Set $f(x) = \operatorname*{Lim}_{n \to \infty} f_n(x)$ or 0 according as this limit exists or not.

Clearly f satisfies properties (1) and (2) for $\mathcal{F}^*$. We must show that f satisfies (3), that $\| f \| < \infty$, and that $\| f_n - f \| \to 0$. Let $g \in C_0^+(G)$.

Iterating the parallelogram identity for $\mathcal{V}$, we see that

$$\int \| f_r(x) - f_{r+k}(x) \|^2 g(x) \, dx \leqq \sum_{j=1}^\infty 2^j \int \| f_{r+j-1}(x) - f_{r+j}(x) \|^2 g(x) \, dx$$
$$\leqq \sum_{j=1}^\infty 2^j \| f_{r+j-1} - f_{r+j} \|^2 \| \tau g \|_M < 2^{-2r+2} \| \tau g \|_M.$$

By Fatou's lemma, $\int \| f_r(x) - f(x) \|^2 g(x) \, dx \leqq 2^{-2r+2} \| \tau g \|_M$. Letting K be compact in G and setting $g = 1$ on K, we see that $\| f_r(\cdot) - f(\cdot) \|^2$ is integrable on K. Hence $f \in \mathfrak{F}^*$. Letting g be arbitrary in $C_0^+(G)$, we see that $\| f_r - f \| \leqq 2^{-2r+2}$, whence $f \in \mathfrak{F}$. Finally, $\| f_r - f \| \to 0$.

The following is a restricted form of Bruhat's version ([3], § 4) of a map first introduced by Mackey ([10], § 3). Let $f \in C_0(G)$ and $v \in \mathfrak{V}$. Form

$$\epsilon(f,v)(x) = \int_\Gamma \delta(\xi)^{-\frac{1}{2}} \Delta(\xi)^{\frac{1}{2}} f(\xi x) L_{\xi^{-1}} v \, d\xi.$$

The support of $\epsilon(f,v)$ is contained in ΓK if the support of f is K. Letting $\mathfrak{F}_0$ denote the subspace of $\mathfrak{F}^*$ consisting of functions which are continuous and have compact support modulo Γ, we have $\mathfrak{F}_0 \subseteq \mathfrak{F}$. Clearly $\epsilon(f,v) \in \mathfrak{F}_0$ and is bilinear. Two important facts about ϵ are summarized in the following lemma (cf. [10], Lemma 3.1 and 3.5).

LEMMA 2. (a) *If K is the support of f, $\| \epsilon(f,v) \| \leqq \Lambda_K \| f \|_G \| v \|$.* (b) *If $\mathfrak{D}$ is total in $\mathfrak{V}$, then $\epsilon(C_0(G) \times \mathfrak{D})$ is total in $\mathfrak{H}$.*

Proof. (a) Choose $h \in C_0(G)$ so that $\tau h = 1$ on $\pi(K)$. Let $g \in \mathfrak{F}$. Then

$$\begin{aligned}(\epsilon(f,v), g) &= \int_G h(x)(\epsilon(f,v)(x), g(x))\,dx \\ &= \int_G \int_\Gamma h(x)\delta(\xi)^{-\frac{1}{2}}\Delta(\xi)^{\frac{1}{2}} f(\xi_x)(L_{\xi^{-1}}v, g(x))\,d\xi dx.\end{aligned}$$

Using the Fubini theorem and the invariance properties of Haar measure, this becomes $\int_G \int_\Gamma h(\xi x) f(x)(v, g(x))\,d\xi dx = \int_G f(x)(v, g(x))\,dx$ by the choice of h. Lemma 1 and the Schwarz inequality give $|(\epsilon(f,v), g)| \leqq \Lambda_K \| f \|_G \| g \| \| v \|$ and our result follows.

(b) Suppose $(\epsilon(f,v), g) = 0$ for all $f \in C_0(G)$, $v \in \mathfrak{D}$.

The calculation in (a) shows that for each $v \in \mathfrak{D}$, $(v, g(\cdot)) = 0$ l. a. e. Using [2], Proposition 10, p. 193, we see that $g(\cdot) = 0$ l. a. e.

Remark. If G is a Lie group, the above proof shows that $\epsilon(C_0^\infty(G) \times \mathfrak{V})$ is total in $\mathfrak{H}$.

For any function f on G, define $R_y f$ by $(R_y f)(x) = f(xy)$. Clearly R_y carries $\mathfrak{F}^*$ into $\mathfrak{F}^*$. We assert that $\| R_y f \| = \| f \|$ for $y \in G$, $f \in \mathfrak{F}^*$. In fact, let $g \in C_0(G)$. Then

$$\begin{aligned}\int_M (\tau g)(p)\,d\mu_{R_y f}(p) &= \int_G \| (R_y f)(x) \|^2 g(x)\,dx \\ &= \int_G \| f(x) \|^2 (R_{y^{-1}} g)(x)\,dx = \int_M (\tau R_{y^{-1}} g)(p)\,d\mu_f(p) \\ &= \int_M (R'_{y^{-1}} \tau g)(p)\,d\mu_f(p),\end{aligned}$$

where $(R'_y h)(p) = h(py)$ for any function h on M and any $y \in G$. Taking the sup over all g such that $0 \leqq \tau g \leqq 1$, we have our assertion.

For $y \in G$, let $U^L{}_y$ be the unitary map of $\mathfrak{H}$ onto itself defined by R_y.

PROPOSITION 2. *The map U^L sending $y \to U^L{}_y$ is a continuous unitary representation of G in $\mathfrak{H}$.*

Proof. The representation property is clear. For continuity, let $f, g \in \mathfrak{F}_0$ and let N be a compact neighborhood of e in G. The supports of all the measures $\mu_{U_y f, g}$, $y \in N$, are contained in some common compact subset K of M. Choose $h \in C_0(G)$ so that $\tau h = 1$ on K. Then, for $y \in N$,

$$(U_y f, g) = \int_G h(x)(f(xy), g(x))\,dx,$$

which is a continuous function of y by standard theorems on integration. Our result follows because $\mathfrak{F}_0$ is dense in $\mathfrak{F}$ by Lemma 2.

U^L is called the *representation of G induced by L*. If it is not clear from the context what group is being up to, we shall write ${}_G U^L$.

Remark. In case G and M are separable, our definition of U^L and Mackey's ([10]) are equivalent. In fact, let ν be a quasi-invariant measure on M defined by a ρ-function ρ ([10]), Lemma 1.4). If $f \in \mathfrak{F}_0$, it is readily seen that $\rho^{-\frac{1}{2}} f \in {}^{\mu}\mathfrak{H}^L$ ([10]), § 2) and that the map $f \to \rho^{-\frac{1}{2}} f$ is isometric. The image of $\mathfrak{F}_0$ under this map is easily seen to satisfy the conditions of Lemma 3.3 in [10]. Because of that lemma and our Lemma 2, the map extends to a unitary map of $\mathfrak{H}$ onto ${}^{\mu}\mathfrak{H}^L$, which sets up the required equivalence. We note that our definition of induced representation is fixed once Haar measure has been fixed in G and Γ. Moreover, for different choices of Haar measure we obtain the same $\mathfrak{H}$ with the norm changed by a multiplicative constant. Thus the problem in [10] of showing that all ways of defining the induced representation are equivalent is trivialized.

We end this section by proving the theorem on induction in stages:

THEOREM 1. *Let Γ_1 and Γ_2 be closed subgroups of G with $\Gamma_1 \subseteq \Gamma_2$. Let L be a unitary representation of Γ_1 on $\mathfrak{V}$ and denote the inductions of L to Γ_1 and G by M and U respectively. Then U is unitarily equivalent to U^M.*

Proof. Let δ_1, δ_2, and Δ be the modular functions for Γ_1, Γ_2, and G respectively. Let $\mathfrak{F}^{(1)}$, $\mathfrak{F}^{(2)}$, and $\mathfrak{F}$ denote the spaces for the inductions from Γ_1 to Γ_2, Γ_2 to G, and Γ_1 to G respectively, corresponding to the space $\mathfrak{F}$ in our construction. Let $f \in \mathfrak{F}_0$ with support in $\Gamma_1 K$, compact. For $\eta \in \Gamma_2$, $x \in G$, set $\hat{f}(\eta, x) = \delta_2(\eta)^{-\frac{1}{2}} \Delta(\eta)^{\frac{1}{2}} f(\eta x)$. Let x be fixed. Then

$$\hat{f}(\xi\eta, x) = \delta_1(\xi)^{\frac{1}{2}} \delta_2(\xi)^{-\frac{1}{2}} L_\xi \hat{f}(\eta, x), \quad \xi \in \Gamma_1, \eta \in \Gamma_2.$$

Moreover $\hat{f}(\cdot, x)$ is continuous with support in $\Gamma_1(Kx^{-1} \cap \Gamma_2)$. Thus $\hat{f}(\cdot, x)$ is a member of $\mathfrak{F}^{(1)}{}_0$, which we denote by $\hat{f}(x)$. Now

$$\hat{f}(\eta, \zeta x) = \delta_2(\zeta)^{\frac{1}{2}}\Delta(\zeta)^{-\frac{1}{2}}\hat{f}(\eta\zeta, x)$$

for $\eta, \zeta \in \Gamma_2$, $x \in G$, so that $\hat{f}(\zeta x) = \delta_2(\zeta)^{\frac{1}{2}}\Delta(\zeta)^{-\frac{1}{2}}M_\zeta \hat{f}(x)$. The support of $\hat{f}(\cdot)$ is in $\Gamma_2 K$. To prove continuity, let N be a compact neighborhood of e in G and choose $h \in C_0(G)$ so that $\int_{\Gamma_1} h(\xi x)\,d\xi = 1$ on $\Gamma_1 KN$. Then $\int_{\Gamma_1} h(\xi\eta x)\,d\xi = 1$ for $\eta \in \Gamma_1(KNx^{-1} \cap \Gamma_2)$. Hence

$$\begin{aligned}\| \hat{f}(x) - \hat{f}(y) \|^2 &= \int_{\Gamma_2} h(\eta x) \| \hat{f}(\eta, x) - \hat{f}(\eta, y) \|^2\, d\eta \\ &= \int_{\Gamma_2} \delta_2(\eta)^{-1}\Delta(\eta) h(\eta x) \| f(\eta x) - f(\eta y) \|^2\, d\eta\end{aligned}$$

whenever $y^{-1}x \in N$, and the continuity of $\hat{f}$ follows from the uniform continuity of f on compact sets. Thus $\hat{f}(\cdot)$ is a member of $\mathfrak{F}^{(2)}{}_0$, which we denote by $\hat{f}$. Now $\| \hat{f}(x) \|^2 = \int_{\Gamma_2} \delta_2(\eta)^{-1}\Delta(\eta) h(\eta x) \| f(\eta x) \|^2\, d\eta$. Choose $k \in C_0(G)$ so that $\int_{\Gamma_2} k(\eta x)\, dy = 1$ on $\Gamma_2 K$. Then, using the Fubini theorem and the invariance of Haar measure,

$$\begin{aligned}\| \hat{f} \|^2 &= \int_G k(x) \| \hat{f}(x) \|^2\, dx \\ &= \int_G \int_{\Gamma_2} k(x) \delta_2(\eta)^{-1}\Delta(\eta) h(\eta x) \| f(\eta x) \|^2\, d\eta dx \\ &= \int_{\Gamma_2} \int_G k(\eta^{-1}x) \delta_2(\eta)^{-1} h(x) \| f(x) \|^2\, dx d\eta \\ &= \int_G h(x) \| f(x) \|^2 [\int_{\Gamma_2} k(\eta x)\, d\eta]\, dx = \| f \|^2\end{aligned}$$

by the choice of h and k. Thus $f \to \hat{f}$ is an isometry of $\mathfrak{F}_0$ into $\mathfrak{F}^{(2)}{}_0$.

We next assert that the image of $\mathfrak{F}_0$ in $\mathfrak{F}^{(2)}{}_0$ is dense. Let $g \in C_0(\Gamma_2)$, $h \in C_0(G)$, $v \in \mathfrak{V}$, and set $k(x) = \int_{\Gamma_2} \delta_2(\zeta)^{-\frac{1}{2}}\Delta(\zeta)^{\frac{1}{2}} g(\zeta^{-1}) h(\zeta x)\, d\zeta \in C_0(G)$. Then

$$\epsilon(k, v)(x) = \int_{\Gamma_1} \int_{\Gamma_2} \delta_1(\xi)^{-\frac{1}{2}}\delta_2(\zeta)^{-\frac{1}{2}}\Delta(\zeta\xi)^{\frac{1}{2}} g(\zeta^{-1}) h(\zeta\xi x) L_{\xi^{-1}} v\, d\zeta d\xi \quad \text{so that}$$

$$\begin{aligned}\epsilon(k, v)\hat{}\,(\eta, x) &= \int_{\Gamma_1} \int_{\Gamma_2} \delta_1(\xi)^{-\frac{1}{2}}\delta_2(\zeta\eta)^{-\frac{1}{2}}\Delta(\zeta\xi\eta)^{\frac{1}{2}} g(\zeta^{-1}) h(\zeta\xi\eta x) L_{\xi^{-1}} v\, d\zeta d\xi \\ &= \int_{\Gamma_1} \int_{\Gamma_2} \delta_1(\xi)^{-\frac{1}{2}}\delta_2(\zeta\xi^{-1})^{-\frac{1}{2}}\Delta(\zeta)^{\frac{1}{2}} g(\xi\eta\zeta^{-1}) h(\zeta x) L_{\xi^{-1}} v\, d\zeta d\xi \\ &= \int_{\Gamma_2} \delta_2(\zeta)^{-\frac{1}{2}}\Delta(\zeta)^{\frac{1}{2}} h(\zeta x) [\int_{\Gamma_1} \delta_1(\xi)^{-\frac{1}{2}}\delta_2(\xi)^{\frac{1}{2}} g(\xi\eta\zeta^{-1}) L_{\xi^{-1}} v\, d\xi] d\zeta.\end{aligned}$$

Letting ϵ_1, ϵ_2 be the ϵ-maps for the inductions from Γ_1 to Γ_2, Γ_2 to G respectively, we see that $\epsilon(k,v)^\wedge = \epsilon_2(h,\epsilon_1(g,v))$. By Lemma 2, the set $\epsilon_2(C_0(G)\times\epsilon_1(C_0(\Gamma_2)\times\mathcal{V}))$ is total in $\mathcal{F}^{(2)}$, proving our assertion. Finally, we see that the map $f\rightarrow\hat{f}$ extends to a unitary map of $\mathcal{F}$ onto $\mathcal{F}^{(2)}$ which sets up the desired equivalence.

3. **The representation ∂V.** Let G be a Lie group and let V be a unitary representation of G on the Hilbert space $\mathcal{K}$. Let $X\in\mathfrak{g}$, the left invariant Lie algebra of G, and let $x(\cdot)$ be the one-parameter subgroup of G such that $(Xf)(y)=D_tf(yx(t))|_{t=0}$ for all $f\in C_0^\infty(G)$. $dV(X)$ will denote the skew-adjoint infinitesimal generator of the one-parameter unitary group $V_{x(\cdot)}$ in $\mathcal{K}$. We will denote by $\mathcal{K}_\infty$ the largest submanifold of $\mathcal{K}$ contained in $\bigcap[\operatorname{dom}(dV(X)):X\in\mathfrak{g}]$ and invariant under $dV(\mathfrak{g})$. $\mathcal{K}_\infty$ is invariant under V because $dV(X)V_y=V_ydV((\operatorname{ad}y^{-1})X)$, $X\in\mathfrak{g}$, $y\in G$.

Let ∂V be the restriction of dV to $\mathcal{K}_\infty$.

LEMMA 3. *$\mathcal{K}_\infty$ is dense in $\mathcal{K}$ and ∂V is a representation of $\mathfrak{g}$ in the Lie algebra of all skew symmetric linear transformations of $\mathcal{K}_\infty$ into itself.*

Proof. Let $\mathcal{D}$ be the linear space spanned by all vectors of the form

$$\int f(x)V_x^{-1}v\,dx \text{ for } f\in C_0^\infty(G),\ v\in\mathcal{K}.$$

Gårding has shown ([5]) that $\mathcal{D}\subseteq\bigcap[\operatorname{dom}(dV(X)):X\in\mathfrak{g}]$, is dense in $\mathcal{K}$, and is invariant under all $dV(X)$, and that the restriction δV of dV to $\mathcal{D}$ is a representation of $\mathfrak{g}$. Therefore $\mathcal{D}\subseteq\mathcal{K}_\infty$ and $\mathcal{K}_\infty$ is dense in $\mathcal{K}$. Segal has shown ([13]) that $\delta V(X)$ is essentially skew-adjoint, $X\in\mathfrak{g}$.

Let $X,Y\in\mathfrak{g}$. Then $\partial V(X)+\partial V(Y)\supseteq\delta(X+Y)$ and $[\partial V(X),\partial V(Y)]\supseteq\delta V([X,Y])$. Since the left hand members are skew-symmetric, they must be contained in the closures of the respective right hand members. Restricting these closures to $\mathcal{K}_\infty$, we have our result.

Let $\mathfrak{E}$ be the enveloping algebra of the complexification of $\mathfrak{g}$. Lemma 3 allows us to extend ∂V to be a representation of $\mathfrak{E}$ in the algebra of endomorphisms of $\mathcal{K}_\infty$. If $+$ is the unique involutory conjugate linear anti-automorphism of $\mathfrak{E}$ such that $X^+=-X$ for $X\in\mathfrak{g}$, it is easy to see that $\partial V(X^+)\subseteq\partial V(X)^*$ for $X\in\mathfrak{E}$ (cf. [12]).

LEMMA 4. *Let V^1 and V^2 be unitary representations of G on $\mathcal{K}^1$ and $\mathcal{K}^2$ respectively. Let $A\in\mathfrak{R}(V^1,V^2)$, the space of operators intertwining V^1 and V^2* ([10], § 8). *Then $A\mathcal{K}^1_\infty\subseteq\mathcal{K}^2_\infty$. Moreover $A\partial V^1(X)\subseteq\partial V^2(X)A$ for $X\in\mathfrak{E}$.*

Proof. Let $X \in \mathfrak{g}$ and let $x(\cdot)$ be the one-parameter subgroup of G underlying X. We have $V^2{}_{x(t)}A = AV^1{}_{x(t)}$, $t \in \boldsymbol{R}$. Hence, if $v \in \operatorname{dom}(dV^1(X))$, $Av \in \operatorname{dom}(dV^2(X))$ and $dV^2(X)Av = AdV^1(X)v$; i.e., $dV^2(X)A \supseteq AdV^1(X)$. We conclude that $A\mathcal{K}^1{}_\infty \subseteq [\operatorname{dom}(dV^2(X)). X \in \mathfrak{g}]$ and that $A\mathcal{K}^1{}_\infty$ is invariant under $dV^2(\mathfrak{g})$. Therefore $A\mathcal{K}^1{}_\infty \subseteq \mathcal{K}^2{}_\infty$. It follows that $A\partial V^1(X) \subseteq \partial V^2(X)A$ for $X \in \mathfrak{g}$. The same statement for $X \in \mathfrak{E}$ is immediate.

In the next two lemmas, we return to the situation of Section 2. G is a Lie group. We shall denote by $\mathfrak{F}_0{}^\infty$ the space of all infinitely strongly differentiable functions in $\mathfrak{F}_0$.

LEMMA 5. $\mathfrak{F}_0{}^\infty \subseteq \mathfrak{H}_\infty$. *Moreover* $\partial U^L(X)f = Xf$ *for all* $X \in \mathfrak{E}$, $f \in \mathfrak{F}_0{}^\infty$.

Proof. Let $X \in \mathfrak{g}$ and let $x(\cdot)$ be the one-parameter subgroup of G underlying X. Let $f \in \mathfrak{F}_0{}^\infty$. There is a compact subset K of M such that $\pi^{-1}(K)$ contains the supports of Xf and $R_{x(t)}f$, $|t| \leqq 1$. Choose $h \in C_0{}^+(G)$ such that $\tau h = 1$ on K. Then

$$\| t^{-1}(U^L{}_{x(t)}f - f) - Xf \|^2 = \int h(y) \| t^{-1}(f(yx(t)) - f(y)) - (Xf)(y) \|^2 dy$$

for $0 < |t| \leqq 1$. But

$$\begin{aligned} \| t^{-1}(f(yx(t)) - f(y)) - (Xf)(y) \|^2 &\leqq 2 \| t^{-1}(f(yx(t)) - f(y)) \|^2 \\ &+ 2 \| (Xf)(y) \|^2 \leqq 2 \sup[\| (Xf)(yx(t')) \|^2 : |t'| \leqq 1] \\ &+ 2 \| (Xf)(y) \|^2 \leqq 4 \| (Xf)(y) \|_G{}^2. \end{aligned}$$

The bounded convergence theorem applies to show that $dU^L(X)f = Xf$. From this the lemma follows exactly as in Lemma 4.

LEMMA 6. *Let* $f \in C_0{}^\infty(G)$, $v \in \mathfrak{V}$. *Then* $\epsilon(f, v) \in \mathfrak{H}_\infty$. *Moreover* $\partial U^L(X)\epsilon(f, v) = \epsilon(Xf, v)$ *for all* $X \in \mathfrak{E}$.

Proof. Let $X \in \mathfrak{g}$ and let $x(\cdot)$ be the one-parameter subgroup of G underlying X. There is a compact subset K of G containing the supports of Xf and $R_{x(t)}f$, $|t| \leqq 1$. Then

$$\begin{aligned} &\| t^{-1}(U_{x(t)}\epsilon(f, v) - \epsilon(f, v)) - \epsilon(Xf, v) \| \\ &\quad = \| \epsilon(t^{-1}(R_{x(t)}f - f) - Xf, v) \| \leqq \Delta_K \| t^{-1}(R_{x(t)}f - f) - Xf \|_G \| v \| \end{aligned}$$

if $0 < |t| \leqq 1$, using Lemma 2 and the fact that $R_y \circ \epsilon = \epsilon \circ (R_y \times I)$, $y \in G$. We conclude that $dU^L(X)\epsilon(f, v) = \epsilon(Xf, v)$, and the lemma follows as in Lemma 4.

COROLLARY. *Let* $f \in C_0^\infty(G)$, $X \in \mathfrak{G}$. *Then* $v \rightarrow \partial U^L(X)\epsilon(f,v)$ *is a bounded linear map from* $\mathcal{V}$ *to* $\mathcal{H}$.

Proof. From Lemmas 2 and 6.

4. Certain elliptic operators. Let $\mathcal{V}_i$ be a finite dimensional Hilbert space and $\Gamma_i = (X_i, \mathfrak{F}_i, \mu_i)$ be a measure space, $i = 1,2$ (μ_i is a measure defined on the σ-field $\mathfrak{F}_i$ of subsets of X_i). $\mathcal{H}_i = L_2(\Gamma_i; \mathcal{V}_i)$ will then be the Hilbert space of all measurable functions f from X_i to $\mathcal{V}_i$ such that $\| f \| = (\int \| f(x) \|^2 d\mu_i(x))^{\frac{1}{2}} < \infty$ (modulo those for which $\| f \| = 0$). $\mathscr{L}(\mathcal{V}_1; \mathcal{V}_2)$ is also a Hilbert space under the norm $\| T \| = \text{trace } (T^*T)^{\frac{1}{2}}$ so that we can form the Hilbert space $\mathcal{H}_{12} = L_2(\Gamma_1 \times \Gamma_2; \mathscr{L}(\mathcal{V}_1; \mathcal{V}_2))$. If $\sigma \in \mathcal{H}_{12}$ and $f \in \mathcal{H}_2$, then $\sigma(\cdot, f) = \int \sigma(\cdot, x) f(x) d\mu(x)$ is in $\mathcal{H}_1$. Therefore the map $f \rightarrow \sigma(\cdot, f)$ is in $\mathscr{L}(\mathcal{H}_2; \mathcal{H}_1)$. It is easily seen that its (operator) norm is $\leqq \| \sigma \|$. Letting $\mathcal{H}_{21} = L_2(\Gamma_2 \times \Gamma_1; \mathscr{L}(\mathcal{V}_2; \mathcal{V}_1))$, we easily see that the adjoint of $f \rightarrow \sigma(\cdot, f)$, $\sigma \in \mathcal{H}_{12}$, is the map $g \rightarrow \sigma^*(\cdot, g)$ where $\sigma^* \in \mathcal{H}_{21}$ is defined by $\sigma^*(x,y) = \sigma(y,x)^*$ for $(x,y) \in X_2 \times X_1$. The next lemma deals with certain special kernels σ.

LEMMA 7. *Let* X_i *be an open subset of* $\boldsymbol{R}^n$, $\mathfrak{F}_i$ *the Borel field of* X_i, *and* μ_i *Lebesgue measure on* $\mathfrak{F}_i$, $i = 1, 2$. *Let* $\sigma \in \mathcal{H}_{12}$ *have the following properties:* (1) *there is an* $h \in L_2(\boldsymbol{R}^n)$ *such that* $\| \sigma(x,y) \| \leqq h(x-y)$ *for* $(x,y) \in X_1 \times X_2$; (2) *there is a null set* $N \subseteq \boldsymbol{R}^n$ *such that* σ *is continuous on* $[(x,y) \in X_1 \times X_2 \colon x - y \notin N]$. *Then, for all* $f \in \mathcal{H}_2, \sigma(\cdot, f) \in C(X_1; \mathcal{V}_1)$ *and* $\| \sigma(\cdot, f) \|_{X_1} \leqq \| h \| \, \| f \|$.

Proof.

$$\begin{aligned} \| \sigma(x,f) \| &\leqq \int_{X_2} \| \sigma(x,y) \| \, \| f(y) \| \, dy \\ &\leqq \left(\int \| h(x-y) \|^2 \right)^{\frac{1}{2}} \left(\int_{X_2} \| f(y) \|^2 dy \right)^{\frac{1}{2}} = \| h \| \, \| f \|. \end{aligned}$$

Now if $f \in C_0(X_2; \mathcal{V}_2)$, we have $\sigma(x,f) = \int \sigma(x, x+y) f(x+y) dy$. Except for $y \in N$, the function $x \rightarrow \sigma(x, x+y) f(x+y)$ is continuous from X_1 to $\mathcal{V}_1$. Moreover, if B is bounded open subset of X_1 and S is the support of f, then $\| \sigma(x, x+y) f(x+y) \| \leqq h(y) \| f \|_{X_2} \chi_{S+(-B)}(y) \in L_1(\boldsymbol{R}^n)$ for all $x \in B$. Hence the bounded convergence theorem applies to give the continuity of $\sigma(\cdot, f)$ when $f \in C_0(X_2; \mathcal{V}_2)$. The same for general f follows from the estimate

$\| \sigma(\cdot, f) \|_{X_1} \leqq \| h \| \, \| f \|$ for $f \in \mathfrak{H}_2$ and from the fact that $C_0(X_2; \mathfrak{V}_2)$ is dense in $\mathfrak{H}_2$.

Remark. If σ is a kernel of the above type, so is σ^* (with interchange of X_1 and X_2, etc.).

We shall apply this lemma in proving a result on analytic elliptic linear differential operators with coefficients in $\mathcal{L}(\mathfrak{V}; \mathfrak{V})$, $\mathfrak{V}$ a finite dimensional Hilbert space. Let $\boldsymbol{J}_+$ denote the non-negative integers. If $\zeta = (\zeta_1, \cdots, \zeta_n) \in \boldsymbol{R}^n$ and $s = (s_1, \cdots, s_n) \in \boldsymbol{J}_+^n$, we put $\zeta^s = \prod \zeta_i^{s_i}$. Moreover, if $| s | = \sum s_i$, then $\partial^{|s|}/\partial x^s$ will denote the operator $\partial^{s_1}/\partial x_1^{s_1} \cdots \partial^{s_n}/\partial x_n^{s_n}$ on all complex valued $C^{|s|}$ functions defined on open subsets of $\boldsymbol{R}^n$. Let O be an open subset of R^n and let $m \in \boldsymbol{J}_+$. Let $A_s(\cdot) \in C^\omega(O; \mathcal{L}(\mathfrak{V}; \mathfrak{V}))$, $| s | \leqq m$. The analytic linear differential operator $L = \sum_{|s| \leqq m} A_s(\cdot) \partial^{|s|}/\partial x^s$ in O of order m will be called *elliptic* if, for every $x \in O$, $Q(x; \zeta) = \sum_{|s|=m} A_s(x) \zeta^s$ is singular only if $\zeta = 0$. Although this definition of ellipticity is more restrictive than that given in [8], it is independent of basis in $\mathfrak{V}$ and suffices for our purposes.

PROPOSITION 3. *Let L be an analytic elliptic linear differential operator of order m with coefficients in $\mathcal{L}(\mathfrak{V}; \mathfrak{V})$ and defined in the open set O of $\boldsymbol{R}^n$. Suppose $m > n/2$. Let V be an isometry of $L_2(O; \mathfrak{V})$ into a Hilbert space $\mathcal{K}$. Let T be a densely defined operator in $\mathcal{K}$ such that $VC_0^\infty(O; \mathfrak{V}) \subseteq \mathrm{dom}(T)$ and $TVf = VLf$ for $f \in C_0^\infty(O; \mathfrak{V})$. Then:* (1) $V^*(\mathrm{dom}(T^*)) \subseteq C(O; \mathfrak{V})$; (2) *for every compact subset K of O there is a constant C_K such that $\| V^* v \|_K \leqq C_K(\| V^* T^* v \| + \| V^* v \|)$ for all $v \in \mathrm{dom}(T^*)$.*

Proof. We follow closely the proof of Lemma 2.1 in [6] (cf. [15], Theorem 1). Let $x_0 \in O$. Let O_1 be a bounded open neighborhood of x_0 such that L has a fundamental solution H defined on $O_1 \times O_1$ with the properties (see [8], Chapter III): (a) $H \in C^\omega(D; \mathcal{L}(\mathfrak{V}; \mathfrak{V}))$, where

$$D = [(x, y) \in O_1 \times O_1 : x \neq y].$$

(b) $\| H(x, y) \| = O(\| x - y \|^{m-n-\epsilon})$ for all $\epsilon > 0$, where $\| x \|$ is the Euclidean norm of x in $\boldsymbol{R}^n$; (c) for all $y \in O_1$, $LH(\cdot, y) = 0$ on O_1 except at y; (d) $g = L \int H(\cdot, y) g(y) dy$ for all $g \in C_0^\infty(O_1; \mathfrak{V})$. From [8], Chapter VII, we know that $\int H(\cdot, y) g(y) dy \in C^\infty(O_1; \mathfrak{V})$ for all $g \in C_0^\infty(O_1; \mathfrak{V})$. Choose $k \in C_0^\infty(O_1)$ such that $k = 1$ in an open neighborhood O_2 of x_0. Exactly as in [6], we see that

$$g = L\int k(\cdot)H(\cdot,y)g(y)dy + \int L[(1-k(\cdot)H(\cdot,y))]g(y)dy$$

on O_1 for all $g \in C_0^\infty(O_2;\mathfrak{V})$.

For $(x,y) \in O \times O_2$, set $\xi(x,y) = k(x)H(x,y)$ or 0 and set $\eta(x,y) = L_x[(1-k(x))H(x,y)]$ or 0, according as $x \in O_1$ or not. Properties (a) and (c) of H imply that η is a bounded continuous function on $O \times O_2$ and so is a kernel of the type considered in Lemma 7. So is ξ by virtue of properties (a) and (b) of H and the choice of m. Note also that $\xi(\cdot,g) \in C_0^\infty(O;\mathfrak{V})$ whenever $g \in C_0^\infty(O_2;\mathfrak{V})$.

Let $v \in \operatorname{dom}(T^*)$. Then, for all $g \in C_0^\infty(O_2;\mathfrak{V})$, we have

$$(V^*v,g) = (V^*v, L\xi(\cdot,g)) + (V^*v,\eta(\cdot,g)).$$

The first term

$$= (v, VL\xi(\cdot,g)) = (v, TV\xi(\cdot,g)) = (V^*T^*v, \xi(\cdot,g) = (\xi^*(\cdot, V^*T^*v), g),$$

while the second term $= (\eta^*(\cdot,V^*v),g)$. We conclude that $(V^*v)(x) = \xi^*(x,V^*T^*v) + \eta^*(x,V^*v)$ for almost all $x \in O_2$. From Lemma 7 and the remark following it we conclude the truth of our assertions in O_2. The general statements are immediate because of the arbitrariness of x_0.

We now apply Proposition 3 to prove the key result needed for our intertwining number theorems. A member of E will be called *elliptic* if it is elliptic regarded as a left invariant (analytic) linear differential operator. We use the notation of Sections 2 and 3.

THEOREM 2. *Suppose* $\dim \mathfrak{V} < \infty$. *Then* $\mathfrak{H}_\infty \subseteq C(G;\mathfrak{V})$. *Suppose, moreover, that* X_0 *is an elliptic element of* $\mathfrak{E}$ *of order* $m > n/2$, *where* $n = \dim M$. *Then for every compact subset* K *of* G *there is a constant* C_K *such that* $\| g \|_K \leqq C_K(\| \partial U^L(X_0)g \| + \| g \|)$ *for all* $g \in \mathfrak{H}_\infty$.

Proof. Clearly there is nothing to prove if $n = 0$ (in fact, in this case, the assumptions of ellipticity and order are unnecessary—we may take $X_0 = 0$). So assume $n \geqq 1$. Let $p_0 \in M$ and let ϕ be a C^ω diffeomorphism from the open unit sphere O_1 of $\boldsymbol{R}^n$ to an open neighborhood of p_0 in M over which there is defined a C^ω cross-section α into G. Set $\beta = \alpha \circ \phi$ and $\psi = \phi^{-1} \circ \pi$. The map ω of $\Gamma \times O_1$ onto $\psi^{-1}(O_1)$ defined by $\omega(\xi,p) = \xi\beta(p)$ is a C^ω diffeomorphism. Let μ be right Haar measure on G and set $\nu = \mu \circ \omega$, a Radon measure in $\Gamma \times O_1$. Let λ be the Cartesian product of right Haar measure in Γ and Lebesgue measure in O_1. If γ is the density of ν with respect to λ, clearly $0 < \gamma \in C^\omega(\Gamma \times O_1)$. For $\xi_1 \in \Gamma$ and $(\xi,p) \in \Gamma \times O_1$, set $\xi_1(\xi,p) = (\xi_1\xi,p)$.

Then it is clear that $\nu(\xi_1 S) = \Delta(\xi_1)\nu(S)$ and $\lambda(\xi_1 S) = \delta(\xi_1)\lambda(S)$ for all $\xi_1 \in \Gamma$ and all Borel $S \subseteq \Gamma \times O_1$. It follows that $\gamma(\xi_1\xi, p)\delta(\xi_1) = \gamma(\xi, p)\Delta(\xi_1)$ for $\xi, \xi_1 \in \Gamma$ and $p \in O_1$, so that $\gamma(e, p) = \delta(\xi)\Delta(\xi)^{-1}\gamma(\xi, p)$ for $(\xi, p) \in \Gamma \times O_1$.

Now let $O = (\frac{1}{2})O_1$ and choose $h \in C_0^+(\psi^{-1}(O_1))$ so that $\tau h = 1$ on $\phi(O)$. If $f \in L_2(O; \mathfrak{V})$, define $\hat{f}$ on G by

$$\hat{f}(x) = \gamma(e, \psi(x))^{-\frac{1}{2}}\delta(x\beta(\psi(x))^{-1})^{\frac{1}{2}}\Delta(x\beta(\psi(x))^{-1})^{-\frac{1}{2}}L_{x\beta(\psi(x))^{-1}}f(\psi(x))$$

or 0 according as $x \in \psi^{-1}(O)$ or not. Clearly $\hat{f}$ satisfies properties (1) and (2) in the definition of $\mathcal{F}^*$ (Section 2). Moreover

$$\int_O \| f(p) \|^2 dp$$
$$= \int_O \int_\Gamma \| f(p) \|^2 \gamma(e, p)^{-1}\delta(\xi)\Delta(\xi)^{-1}\gamma(\xi, p)h(\xi\beta(p))\, d\xi dp$$

by the choice of h; and this, by the Fubini theorem and the definitions of γ and $\hat{f}$, is

$$\int_{\Gamma\times O} \| \hat{f}(\xi\beta(p)) \|^2 h(\xi\beta(p))\, d\nu(\xi, p) = \int_G \| \hat{f}(x) \|^2 h(x)\, dx.$$

This shows that $\| \hat{f}(\cdot) \|^2$ is integrable on compact subsets of $[x\colon h(x) > 0]$ and therefore of $\Gamma[x\colon h(x) > 0] \supseteq [x\colon (\tau h)(\pi(x)) > \frac{1}{2}] \supseteq [x\colon \hat{f}(x) \neq 0]$. Therefore $\hat{f}$ is locally integrable on G and $\| \hat{f} \| = \| f \|_2$. Setting $Vf = \hat{f}$ for $f \in L_2(O; \mathfrak{V})$, we see that V is an isometry of $L_2(O; \mathfrak{V})$ into $\mathcal{H}$. A similar calculation shows that $(V^*g)(\cdot) = \lambda(e, \cdot)^{\frac{1}{2}}g(\beta(\cdot))$, a.e. in O, for $g \in \mathcal{F}$. It is clear that V maps $C_0^\infty(O; \mathfrak{V})$ onto the subspace of $\mathcal{F}_0^\infty$ consisting of functions whose supports $\subseteq \psi^{-1}(O)$, a subspace $\subseteq \operatorname{dom}(\partial U^L(X))$ and invariant under $\partial U^L(X)$ for all $X \in \mathfrak{G}$.

If f is a complex valued C^ω function defined on an open subset of $\Gamma \times O$, we set $\omega f = f \circ \omega^{-1}$. X_0^+ is elliptic. The analytic elliptic linear differential operator $\omega^{-1} \circ X_0^+ \circ \omega$ we write as $L_0 = \sum_{|r|+|s| \leqq m} a_{rs}(\xi, p)\partial^{|r|+|s|}/\partial\xi^r\partial p^s$ in some neighborhood of $\{e\} \times O$ adapted to the Cartesian decomposition of $\Gamma \times O$. Then, if $f \in C_0^\infty(O; \mathfrak{V})$, we have

$$(V^*\partial U^L(X_0^+)Vf)(p) = \gamma(e, p)^{\frac{1}{2}}(X_0^+f)(\beta(p))$$
$$= \sum_{|r|+|s| \leqq m} \gamma(e, p)^{\frac{1}{2}}a_{rs}(e, p)$$
$$[(\partial^{|r|}/\partial\xi^r)(\delta(\xi)^{\frac{1}{2}}\Delta(\xi)^{-\frac{1}{2}}L_\xi)]_{\xi=e}(\partial^{|s|}/\partial p^s)(\gamma(e, p)^{-\frac{1}{2}}f(p))$$
$$= \sum_{|s| \leqq m} A_s(p)(\partial^{|s|}/\partial p^s)f(p),$$

where the $A_s \in C^{\omega}(O;\mathscr{L}(\mathcal{V};\mathcal{V}))$. The operator $L=\sum_{|s|\leqq m} A_s(\cdot)\partial^{|s|}/\partial p^s$ is *elliptic.* In fact, if $|s|=m$, $A_s(p)=a_{0s}(e,p)I$. Hence

$$Q(p;\zeta)=\sum_{|s|=m} A_s(p)\zeta^s=(\sum_{|s|=m} a_{0s}(e,p)\zeta^s)I,$$

which is singular only if $\zeta=0$ by the ellipticity of L_0.

Proposition 3 says: (1) if $f\in\mathcal{H}_{\infty}$, then $V^{*}f\in C(O;\mathcal{V})$; (2) for any compact subset K_0 of O there exists a constant C'_{K_0} such that $\| V^{*}f\|_{K_0}\leqq C'_{K_0}$ $(\|\partial U^L(X_0)f\|+\|f\|)$ (we here make use of the fact that $\partial U^L(X_0)$ $\subseteq \partial U^L(X_0{}^{+})^{*}$). Thus $f(\beta(\cdot))$ is continuous on O and we conclude that

$$x\rightarrow f(x)=\delta(x\beta(\psi(x))^{-1})^{\frac{1}{2}}\Delta(x\beta(\psi(x))^{-1})^{-\frac{1}{2}}L_{x\beta(\psi(x))^{-1}}f(\beta(\psi(x)))$$

is continuous on $\psi^{-1}(O)$. From the arbitrariness of p_0 and the existence of elliptic members of $\mathfrak{E}$ of arbitrarily high order (see, e.g., [15]) we conclude the truth of the first assertion of our theorem. Moreover, the second assertion holds for any compact $K\subseteq\psi^{-1}(O)$: we need only take $C_K=C'_{\psi(K)}$.

$$\text{LUB}[\delta(x\beta(\psi(x))^{-1})^{-\frac{1}{2}}\Delta(x\beta(\psi(x))^{-1})^{-\frac{1}{2}}\gamma(e,\psi(x))^{-\frac{1}{2}}\,\|L_{x\beta(\psi(x))^{-1}}\|: x\in K].$$

The second assertion for general K follows easily from this and the arbitrariness of p_0.

5. An intertwining number theorem. Let Γ_1 and Γ_2 be closed subgroups of the Lie group G with modular functions δ_1 and δ_2 respectively. Let $L^{(i)}$ be a unitary representation of Γ_i on the Hilbert space $\mathcal{V}_i$, $i=1,2$. $U^{L^{(i)}}$ operates on $\mathcal{H}^{(i)}$. We shall assume that $\dim\mathcal{V}_2<\infty$. For each $A\in\mathcal{R}(U^{L^{(1)}},U^{L^{(2)}})$ we define a linear map r_A from $C_0{}^{\infty}(G)$ to the linear maps of $\mathcal{V}_1$ into $\mathcal{V}_2$ as follows: for each $f\in C_0{}^{\infty}(G)$ and $v\in\mathcal{V}_1$, set $r_A(f)v$ $=(A\epsilon(f,v))(e)$. This definition makes sense: in fact, $\epsilon(f,v)\in\mathcal{H}^{(1)}{}_{\infty}$ by Lemma 6, which implies that $A\epsilon(f,v)\in\mathcal{H}^{(2)}{}_{\infty}$ by Lemma 4, so that $A\epsilon(f,v)$ $\in C(G;\mathcal{V})$ by Theorem 1 and the value of $A\epsilon(f,v)$ at e is well determined. For $(\xi_1,\xi_2)\in\Gamma_1\times\Gamma_2$ and for any function f on G, we set $(\rho_{\xi_1,\xi_2}f)=f(\xi_1{}^{-1}x\xi_2)$, $x\in G$. We may now state our main theorem.

THEOREM 3. *Let X_0 be an elliptic element of $\mathfrak{E}$ of order $>\frac{1}{2}\dim(G/\Gamma_3)$. For $f\in C_0{}^{\infty}(G)$, set $\|f\|_{X_0}=\|X_0f\|_G+\|f\|_G$. For each relatively compact open set O of G, give $C_0{}^{\infty}(O)$ the topology induced by $\|\cdot\|_{X_0}$; give $C_0{}^{\infty}$ the corresponding inductive limit topology* [1]. *Let $\mathcal{M}=$ the subspace of maps $Z\in\mathscr{L}(C_0{}^{\infty}(G);\mathscr{L}(\mathcal{V}_1;\mathcal{V}_2))$ such that*

$$Z(\rho_{\xi_1,\xi_2}f)=\delta_1(\xi_1)^{\frac{1}{2}}\delta_2(\xi_2)^{\frac{1}{2}}\Delta(\xi_1\xi_2{}^{-1})^{\frac{1}{2}}L^{(2)}{}_{\xi_2}Z(f)L^{(1)}{}_{\xi_1{}^{-1}}$$

for all $(\xi_1, \xi_2) \in \Gamma_1 \times \Gamma_2$ *and all* $f \in C_0^\infty(G)$. *Then the map* $A \to r_A$ *is a faithful linear map of* $\mathfrak{R}(U^{L^{(1)}}, U^{L^{(2)}})$ *into* $\mathcal{M}$.

Proof. Let $v \in \mathfrak{V}_1$, $A \in \mathfrak{R}(U^{L^{(1)}}, U^{L^{(2)}})$, and $f \in C_0^\infty(O)$, O a relatively compact open subset of G. By Theorem 2,

$$\| r_A(f)v \| \leqq C_{\{e\}}(\| \partial U^{L^{(2)}}(X_0)A\epsilon(f, v) \| + \| A\epsilon(f, v) \|).$$

But $\partial U^{L^{(2)}}(X_0)A\epsilon(f, v) = A\partial U^{L^{(1)}}(X_0)\epsilon(f, v) = A\epsilon(X_0 f, v)$ by Lemmas 4 and 6. Therefore

$$\begin{aligned} \| r_A(f)v \| &\leqq C_{\{e\}} \| A \| (\| \epsilon(X_0 f, v) \| + \| \epsilon(f, v) \|) \\ &\leqq C_{\{e\}} \| A \| \Lambda_{\bar{O}} \| v \| (\| X_0 f \|_G + \| f \|_G) = C_{\{e\}} \Lambda_{\bar{O}} \| A \| \, \| f \|_{X_0} \| v \|. \end{aligned}$$

This proves that $r_A \in \mathcal{L}(C_0^\infty(G); \mathcal{L}(\mathfrak{V}_1; \mathfrak{V}_2))$.

Suppose $r_A = 0$. Let $f \in C_0^\infty(G)$ and $v \in \mathfrak{V}_1$. For all $x \in G$ we have

$$(A\epsilon(f, v))(x) = (U^{L^{(2)}}{}_x A\epsilon(f, v))(e) = (AU^{L^{(1)}}{}_x \epsilon(f, v))(e) = r_A(R_x f)v = 0$$

because $U^{L^{(1)}}{}_x \circ \epsilon = \epsilon \circ (R_x \times I)$. Therefore A is 0 on $\epsilon(C_0^\infty(G) \times \mathfrak{V}_1)$, a total subset of $\mathfrak{H}^{(1)}$ by the remark following Lemma 2.

To show that $r_A \in \mathcal{M}$, let $f \in C_0^\infty(G)$, $v \in \mathfrak{V}_1$, and $(\xi_1, \xi_2) \in \Gamma_1 \times \Gamma_2$. Then $r_A(\rho_{\xi_1, \xi_2} f)v = r_A(R_{\xi_2}\rho_{\xi_1, e} f)v = (A\epsilon(\rho_{\xi_1, e} f, v)(\xi_2)$ exactly as above, and this $= \delta_2(\xi_2)^{\frac{1}{2}}\Delta(\xi_2)^{-\frac{1}{2}}L^{(2)}{}_{\xi_2} r_A(\rho_{\xi_1, e} f)$ by property (2) for functions of $\mathfrak{F}^*$. On the other hand,

$$\begin{aligned} \epsilon(\rho_{\xi_1, e} f, v)(x) &= \int_{\Gamma_1} \delta_1(\xi)^{-\frac{1}{2}}\Delta(\xi)^{\frac{1}{2}} f(\xi_1^{-1}\xi x) L^{(1)}{}_{\xi^{-1}} v \, d\xi \\ &= \int_{\Gamma_1} \delta_1(\xi_1\xi)^{-\frac{1}{2}}\Delta(\xi_1\xi)^{\frac{1}{2}} f(\xi x) L^{(1)}{}_{\xi^{-1}\xi_1^{-1}} v \delta_1(\xi_1) \, d\xi \\ &= \delta_1(\xi_1)^{\frac{1}{2}}\Delta(\xi_1)^{\frac{1}{2}}\epsilon(f, L^{(1)}{}_{\xi_1^{-1}} v)(x). \end{aligned}$$

Therefore $r_A \in \mathcal{M}$.

If V and W are representations of G, dim $\mathfrak{R}(V, W)$ is called the ***intertwining number*** of V and W and is denoted by $I(V, W)$ ([10]). Theorem 3 has the following consequence.

COROLLARY. $I(U^{L^{(1)}}, U^{L^{(2)}}) \leqq \dim \mathcal{M}$.

6. Inducing from compact subgroups.

For notation, terminology, and facts about direct integrals of Hilbert spaces, we refer the reader to [4]. Let X be a separable locally compact space and let μ be a positive Radon measure for X. Let $t \to \mathfrak{H}(t)$ be a field of separable Hilbert spaces and let G be a separable locally compact group. A *field of (unitary) representations of* G is a map which assigns to each $t \in X$ a representation $U(t)$ of G on $\mathfrak{H}(t)$. If $t \to \mathfrak{H}(t)$ is measurable, then $t \to U(t)$ is called *measurable* if $t \to U_x(t)$ is a measurable operator field for each $x \in G$. We know ([10], that $x \to \int^{\oplus} U_x(t)\, d\mu(t)$ is a representation of G on $\int^{\oplus} \mathfrak{H}(t)\, d\mu(t)$, which we denote $\int^{\oplus} U(t)\, d\mu(t)$.

If V and W are representations of $G, J(V, W)$ will denote the dimension of the subspace of all Hilbert-Schmidt operators in $\mathfrak{R}(V, W)$ and will be called the *weak intertwining number* of V and W ([10]).

LEMMA 8. *Let* (X, μ) *be atom free, let* $t \to \mathfrak{H}(t)$ *be a measurable field of Hilbert spaces, and let* $t \to U(t)$ *be a measurable field of representations of the separable locally compact group* G. *Let* V *be a representation of* G *on the separable Hilbert space* $\mathfrak{K}$. *Then the* $Y = [t \in X : J(U(t), V) > 0]$ *is measurable. Moreover* $J(\int^{\oplus} U(t)\, d\mu(t), V) = 0$ *or* ∞ *according as* $\mu(Y) = 0$ *or* > 0.

Proof. Let $\mathfrak{K}'$ be the conjugate space of $\mathfrak{K}$ and let V' be the representation of G in $\mathfrak{K}'$ defined by $V'_x = {}^t V_{x^{-1}}$. The field of Hilbert spaces $t \to \mathfrak{H}(t) \otimes \mathfrak{K}'$ is measurable in a canonical fashion which sets up a unitary equivalence of $\int^{\oplus} (\mathfrak{H}(t) \otimes \mathfrak{K}')\, d\mu(t)$ with $(\int^{\oplus} \mathfrak{H}(t)\, d\mu(t)) \otimes \mathfrak{K}'$ ([4], Ch. II, § 1, Section 8). The field of representations $t \to U(t) \otimes V'$ is then measurable (ibid., § 2, Section 1) and the above unitary equivalence then give a unitary equivalence of $\int^{\oplus} (U(t) \otimes V')\, d\mu(t)$ with $(\int^{\oplus} U(t)\, d\mu(t)) \otimes V'$ (ibid., § 2, Section 6). Now $J(U(t), V) =$ number of times $U(t) \otimes V'$ discretely contains the one-dimensional identity representation of G and similarly for $J(\int^{\oplus} U(t)\, d\mu(t), V)$ ([10], Lemma 8.1). Our lemma now follows from [10], Lemma 13.1.

We are now in a position to prove the main result of this section. We return to the situation of Section 5. Two representations are said to be *disjoint* if no non-0 subrepresentations of one is unitarily equivalent to any subrepresentation of the other.

THEOREM 4. *Suppose that* Γ_1 *and* Γ_2 *are compact and that* $\dim \mathfrak{V}_1$ *and*

$\dim \mathfrak{V}_2 < \infty$. *For each* $x \in G$, *let* ${}_xL^{(2)}$ *be the representation of* $x\Gamma_2 x^{-1}$ *defined by* ${}_xL^{(2)}{}_{\xi} = L^{(2)}{}_{x^{-1}\xi x}$, $\xi \in x\Gamma_2 x^{-1}$. *Suppose that, for locally almost all* $x \in G$, *the restrictions of* $L^{(1)}$ *and* ${}_xL^{(2)}$ *to* $\Gamma_1 \cap (x\Gamma_2 x^{-1})$ *are disjoint. Then* $U^{L^{(1)}}$ *and* $U^{L^{(2)}}$ *are disjoint.*

Proof. Let B be a positive definite bilinear form on $\mathfrak{g}$ invariant under the action of Γ_2 on $\mathfrak{g}$ via the adjoint representation of G on $\mathfrak{g}$. Choose a basis $\{X_i\}$ of $\mathfrak{g}$, orthonormal with respect to B. Exactly as in the discussion of the Casimir operator in [14], Exposé n° 4, we see that $\Delta = \sum X_i^2$ is invariant under $\operatorname{ad} \Gamma_2$ (where the adjoint representation of G has been extended to $\mathfrak{G}$). Moreover $1 - \Delta$ is an elliptic operator on G such that $\int [(1-\Delta)f]\bar{f} \geqq \int |f|^2$ for all $f \in C_0^{\infty}(G)$ (see, for instance, [15]).

Now suppose $U^{L^{(1)}}$ and $U^{L^{(2)}}$ are not disjoint. Then $I(U^{L^{(1)}}, U^{L^{(2)}}) > 0$. Let k be an integer $> (\frac{1}{2})\dim(G/\Gamma_2)$ and set $X_0 = (1-\Delta)^k$. Using X_0 to define $\mathfrak{M}$, we see from the Corollary to Theorem 3 that $\dim \mathfrak{M} > 0$. The map $(x, (\xi_1, \xi_2)) \to \xi_1^{-1} x \xi_2$ of $G \times (\Gamma_1 \times \Gamma_2)$ into G gives the pair $(G, \Gamma_1 \times \Gamma_2)$ the structure of compact analytic transformation group. Hence there is a $Z \in \mathfrak{M}$ and a relatively compact open set O invariant under the action of $\Gamma_1 \times \Gamma_2$ such that $Z \mid C_0^{\infty}(O) \neq 0$. Let l be an integer $> k + (\frac{1}{4})\dim(G)$ and let S be the linear operator in $L_2(O)$ with domain $C_0^{\infty}(O)$ defined by $Sf = (1-\Delta)^l f$, $f \in C_0^{\infty}(O)$. $S \geqq I$ on $C_0^{\infty}(O)$ and so is univalent. We define a representation P of $\Gamma_1 \times \Gamma_2$ on $L_2(O)$ by setting $P_{\xi_1,\xi_2} f = \rho_{\xi_1,\xi_2} f$, $f \in L_2(O)$. Now $\Delta \circ \rho = \rho \circ \Delta$ because Δ is left-invariant and is invariant under $\operatorname{ad} \Gamma_2$. Therefore $SP_{\xi_1,\xi_2} = P_{\xi_1,\xi_2} S$ so that $S^{-1} P_{\xi_1,\xi_2} = P_{\xi_1,\xi_2} S^{-1}$ for all $(\xi_1, \xi_2) \in \Gamma_1 \times \Gamma_2$. Setting $T = ZS^{-1}$, we have a mapping T from a submanifold of $L_2(O)$ to $\mathfrak{L}(\mathfrak{V}_1; \mathfrak{V}_2)$ such that $TP_{\xi_1,\xi_2} f = L^{(2)}{}_{\xi_2}(Tf) L^{(1)}{}_{\xi_1^{-1}}$ for all $f \in \operatorname{dom}(T)$. If we identify $\mathfrak{L}(\mathfrak{V}_1; \mathfrak{V}_2)$ with $\mathfrak{V}_2 \otimes \mathfrak{V}_1'$, we therefore obtain the relation $TP_{\xi_1,\xi_2} = V_{\xi_1,\xi_2} T$, $(\xi_1, \xi_2) \in \Gamma_1 \times \Gamma_2$, where $V_{\xi_1,\xi_2} = L^{(2)}{}_{\xi_2} \otimes L^{(1)}{}_{\xi_1}$ (see [10], § 5). Let $S_1 = (1-\Delta)^l \mid C_0^{\infty}(G)$ and $S_2 = (1-\Delta)^{l-k} \mid C_0^{\infty}(G)$, operators which are symmetric and $\geqq I$ in $L_2(G)$. Applying Proposition 3 to S_1 and S_2, we obtain constants C_1 and C_2 such that $\| f \|_{\bar{o}} \leqq C_1 \| S_1 f \|$ and $\| f \|_{\bar{o}} \leqq C_2 \| S_2 f \|$ for $f \in C_0^{\infty}(G)$. Since $S_1 = S_2 X_0 = S$ on $C_0^{\infty}(O)$, it follows that $\| f \|_{X_0} = \| X_0 f \|_{\bar{o}} + \| f \|_{\bar{o}} \leqq (C_1 + C_2) \| Sf \|$ for all $f \in C_0^{\infty}(O)$. We conclude that T is continuous. Therefore, since $\operatorname{dom}(T)$ is invariant under P, the unique bounded extension T^c of T to $L_2(O)$ which vanishes on $\operatorname{dom}(T)^{\perp}$ belongs to $\mathfrak{R}(P, V) > 0$, and $I(P, V) > 0$. Since $\dim(\mathfrak{V}_2 \otimes \mathfrak{V}_2') < \infty$, it follows that $J(P, V) > 0$.

O, being open and relatively compact, is a separable locally compact space. Let $\mathfrak{X}$ be the space of orbits of O under the action of $\Gamma_1 \times \Gamma_2$. $\mathfrak{X}$ is also a separable locally compact space in the usual topology. We put a Radon measure ν_t on each (compact separable space) $t \in \mathfrak{X}$ as follows: pick a point $x_0 \in t$ and then set $\int f(x)\,d\nu_t(x) = \int_{\Gamma_1 \times \Gamma_2} f(\xi_1^{-1}x_0\xi_2)\,d(\xi_1,\xi_2)$ for all $f \in C(t)$, where Haar measure on $\Gamma_1 \times \Gamma_2$ is normalized so that $\int 1 d(\xi_1,\xi_2) = 1$. The two-sided invariance of Haar measure on compact kroups shows that ν_t is independent of the choice of $x_0 \in t$. We also define a measure μ on $\mathfrak{X}$ by setting $\int_{\mathfrak{X}} f(t)\,d\mu(t) = \int_O (f \circ \pi)(x)\,dx$ for each $f \in C_0(X)$, where π is the usual projection of O on $\mathfrak{X}$. Let $\mathfrak{H}(t) = L_2(t, \nu_t)$, a separable Hilbert space for each $t \in \mathfrak{X}$. Each $f \in C_0(O)$ defines a vector field θf, where $(\theta f)(t) = f \mid t$. If $f, g \in C_0(O)$, then

$$((\theta f)\pi(x)), (\theta g)(\pi(x))) = \int f(\xi_1^{-1}x\xi_2)\bar{g}(\xi_1^{-1}x\xi_2)\,d(\xi_1,\xi_2),$$

whence $t \to ((\theta f)(t), (\theta g)(t))$ is continuous on $\mathfrak{X}$. Moreover, if $\{f_n\}$ is a multiplicatively closed sequence of real functions in $C_0(O)$ which separates the points of O, the Stone-Weierstrass theorem implies that the sequence $\{(\theta f_n)(t)\}$ is total in $\mathfrak{H}(t)$ for all $x \in \mathfrak{X}$. Thus the field of Hilbert spaces $t \to \mathfrak{H}(t)$ has a unique measurable structure such that all vector fields in $G_0 = \theta C_0(O)$ are measurable. Now

$$\begin{aligned} \| \theta f \|^2 &= \int_{\mathfrak{X}} \| (\theta f)(t) \|^2 \,d\mu(t) \\ &= \int_G \int_{\Gamma_1 \times \Gamma_2} | f(\xi_1^{-1}x\xi_2) |^2 \,d(\xi_1,\xi_2)\,dx = \int_G | f(x) |^2 \,dx = \| f \|^2, \end{aligned}$$

for all $f \in C_0(O)$, by the Fubini theorem and the invariance properties of Haar measure on G. Therefore we may identify $L_2(O)$ and $\int^{\oplus} \mathfrak{H}(t)\,d\mu(t)$. For each $t \in \mathfrak{X}$, we define a representation $P(t)$ of $\Gamma_1 \times \Gamma_2$ on $\mathfrak{H}(t)$ by setting $P_{\xi_1,\xi_2}(t)f = \rho_{\xi_1,\xi_2}f$ for $f \in \mathfrak{H}(t)$, $(\xi_1,\xi_2) \in \Gamma_1 \times \Gamma_2$. Since

$$P_{\xi_1,\xi_2}(t)(\theta f)(t) = (\theta P_{\xi_1,\xi_2}f)(t)$$

for each $(\xi_1,\xi_2) \in \Gamma_1 \times \Gamma_2$, $f \in C_0(G)$, and $t \in \mathfrak{X}$, we see that the field of representations $t \to P(t)$ is measurable and that P may be identified with $\int^{\oplus} P(t)\,d\mu(t)$. From Lemma 8 and the fact that V is of finite degree we conclude that the μ-measurable set $Y = [t \in \mathfrak{X} : I(P(t), V) > 0]$ has positive μ-measure.

Fix $t \in \mathfrak{X}$ and pick $x_0 \in t$. The stationary subgroup of x_0 under the action of $\Gamma_1 \times \Gamma_2$ is $\Gamma_{x_0} = [(\xi, x_0^{-1}\xi x_0) : \xi \in \Gamma_1 \cap (x_0 \Gamma_2 x_0^{-1})]$. If $f \in \mathfrak{H}(t)$, define $\chi_t f$ on $\Gamma_1 \times \Gamma_2$ by $(\chi_t f)(\xi_1, \xi_2) = f(\xi_1^{-1} x_0 \xi_2)$. It is easy to see that χ_t identifies $P(t)$ with the representation of $\Gamma_1 \times \Gamma_2$ induced by the one-dimensional identity representation of Γ_{x_0}. Therefore, according to the Frobenius reciprocity theorem for compact groups ([16], pp. 82-83), $I(P(t), V) =$ number of times V restricted to Γ_{x_0} contains the one-dimensional identity representation. But this is just the weak intertwining number of the restrictions of $L^{(1)}$ and ${}_{x_0}L^{(2)}$ to $\Gamma_1 \cap (x_0 \Gamma_2 x_0^{-1})$ ([10], Lemma 8.1). We conclude that the restrictions of $L^{(1)}$ and ${}_{x}L^{(2)}$ to $\Gamma_1 \cap (x \Gamma_2 x^{-1})$ are not disjoint whenever $x \in \pi^{-1}(Y)$, a measurable set of positive measure in the compact set $\bar{O}$. Our theorem is thereby demonstrated.

Remark. As usual (cf. [10]), the intertwining number of the restrictions of $L^{(1)}$ and $x^{L^{(2)}}$ to $\Gamma_1 \cap (x\Gamma_2 x_2^{-1})$ depends only on the $\Gamma_1 : \Gamma_2$ double coset $\Gamma_1 x \Gamma_2$ to which x belongs.

7. An example. Let G be the group of (possibly improper) rigid motions of the Euclidean plane Π, let $P \in \Pi$, and let Γ be the group of (possibly improper) rotations of Π about P. Let $L^{(+)}$ (resp. $L^{(-)}$) be the 1-dimenstional identity representation of Γ (resp. the 1-dimensional representation of Γ which assigns to $\xi \in \Gamma$ the value of $+1$ or -1 as ξ is proper or improper). If T is the subgroup of translations of Π, $G = T\Gamma$ shows that each $\Gamma : \Gamma$ double coset of G contains a member of T. Let $e \neq x \in T$. Then $x\Gamma x^{-1}$ is the group of (possibly improper) rotations about xP, so that $\Gamma \cap (x\Gamma x^{-1})$ is the group consisting of e and reflection in the line through P and xP. Therefore the restrictions of $L^{(-)}$ and ${}_{x}L^{(+)}$ to $\Gamma \cap (x\Gamma x^{-1})$ are disjoint, and by the remark following Theorem 4, this holds for all $x \notin \Gamma$. The same holds if $x \in \Gamma$, for then $\Gamma \cap (x\Gamma x^{-1}) = \Gamma$. From Theorem 4 we conclude that $U^{L^{(+)}}$ and $U^{L^{(-)}}$ are disjoint.

We can derive the same result from Mackey's reciprocity theorem. Since G is a regular semi-direct product of the abelian normal subgroup T and Γ, we may apply the analysis of ([10], § 14) to obtain the following information about the irreducible representations of G. Let $\hat{T}$ be the character group of T and let Γ act on $\hat{T}$ according to the rule $(\chi\xi)(x) = \chi(\xi x \xi^{-1})$ for $\xi \in \Gamma$ $\chi \in \hat{T}$, $x \in T$. Let Ω be the space of orbits of T under Γ and, for each $\omega \in \Omega$, choose $\chi_\omega \in \omega$. Let Γ_ω be the stationary subgroup of χ_ω in Γ. Then each irreducible representation of G is uniquely specified by a $\omega \in \Omega$ and an irreducible representation M of Γ_ω, and conversely. Calling this representation $V^{\omega,M}$, the restriction of $V^{\omega,M}$ to Γ is the representation of Γ induced by M. Now if $\omega = \{e\}$, then $\Gamma_\omega = \Gamma$; and if $\omega \neq \{e\}$, then Γ_ω is the subgroup consisting of the identity and the unique reflection in Γ leaving χ_ω fixed. Moreover if M is an irreducible representation of Γ_ω, we have that ${}_\Gamma U^M$ contains $L^{(\pm)}$ exactly as many times as the restriction of $L^{(\pm)}$ to Γ_ω contains M (the Frobenius reciprocity theorem for compact groups). Thus in any case ${}_\Gamma U^M$ contains $L^{(+)}$ if and only if it does *not* contain $L^{(-)}$. Finally from results of Godement ([7], Theorems 5 and 7) and Kaplansky ([9], Theorem 7), we know that the regular representation of G is of Type I. Therefore Mackey's reciprocity theorem ([11], Theorem 5.1) applies, and we deduce that $U^{L^{(+)}}$ and $U^{L^{(-)}}$ are disjoint.

It is instructive to note that in order to apply Mackey's reciprocity theorems to verify the conclusion of our Theorem 4 in any particular case one needs to know (1) how the regular representation of G decomposes into factors and (2) how these factors, when restricted to Γ_1 and Γ_2, decompose into irreducible representations. Even in so simple a case as the motion group considered above, the machinery needed to dig out these facts is quite formidable. Thus the reciprocity theorem would not seem well suited in general to handle the disjointness question dealt with in Theorem 4.

UNIVERSITY OF CALIFORNIA,
LOS ANGELES.

REFERENCES.

[1] N. Bourbaki, *Espaces vectoriels topologiques*, Chapters I-II, Hermann, Paris, 1953.

[2] ———, *Intégration*, Chapters I-IV, Hermann, Paris, 1952.

[3] F. Bruhat, "Sur les representations induites des groupes de Lie," *Bulletin de la Société Mathématique de France*, vol. 84 (1956), pp. 97-205.

[4] J. Dixmier, *Les algèbres d'opérateurs dans l'espace hilbertien*, Gauthier-Villars, Paris, 1957.

[5] L. Gårding, "Note on continuous representations of Lie groups," *Proceedings of the National Academy of Sciences*, vol. 33 (1947), pp. 331-332.

[6] ———, "Applications of the theory of direct integrals of Hilbert spaces to some integral and differential operators," *Institute for Fluid Dynamics and Applied Mathematics Lecture series*, No. 11, University of Maryland.

[7] R. Godement, "A theory of spherical functions I," *Transactions of the American Mathematical Society*, vol. 73 (1952), pp. 496-556.

[8] F. John, *Plane waves and spherical means*, Interscience, New York, 1955.

[9] I. Kaplansky, "Group algebras in the large," *Tôhoku Mathematical Journal*, vol. 3 (1951), pp. 249-256.

[10] G. W. Mackey, "Induced representations of locally compact groups I," *Annals of Mathematics*, vol. 55 (1952), pp. 101-139.

[11] ———, "Induced representations of locally compact groups II," *ibid.*, vol. 58 (1953), pp. 193-221.

[12] E. Nelson and W. F. Stinespring, "Representation of elliptic operators in an enveloping algebra," *American Journal of Mathematics*, vol. 81 (1959), pp. 547-560.

[13] I. E. Segal, "A class of operator algebras which are determined by groups," *Duke Mathematical Journal*, vol. 18 (1951), pp. 221-265.

[14] *Seminaire "Sophus Lie" 1954-55*, Ecole Normale Superieure, Paris, 1955.

[15] W. F. Stinespring, "Integrability of Fourier transforms for unimodular Lie groups," *Duke Mathematical Journal*, vol. 26 (1959), pp. 123-131.

[16] A. Weil, *L'intégration dans les groupes topologiques et ses applications*, Hermann, Paris, 1940.

ON CHOW VARIETIES OF MAXIMAL, TOTAL, REGULAR FAMILIES OF POSITIVE DIVISORS.*[1]

By J. P. Murre.

Introduction. In this paper we study the Chow variety of a maximal, total, regular family of positive divisors on a non-singular projective variety V. An algebraic family $\mathfrak{U}$ of positive divisors on V is called *maximal* if $\mathfrak{U}$ is not a proper subset of another algebraic family; it is called *total* if for every divisor Y on V, algebraically equivalent to zero, and for an arbitrary fixed (i.e. independent of Y) $X_0 \in \mathfrak{U}$ there exists an $X \in \mathfrak{U}$ such that $Y \sim X - X_0$ ($\sim$ means linear equivalence); finally, it is called *regular* if for every pair $X, X' \in \mathfrak{U}$ we have $l(X) = l(X')$, where $l(X)$ denotes the dimension of the linear system determined by X. These definitions are introduced, and the existence of such families is proved, in [6, 7] (in [6, 7] such families are called maximal, regular, complete instead of maximal, total, regular in this order).

If V is embedded in projective space P^N, then the Chow points are constructed by means of the hyperplanes in P^N, and therefore we must expect that there is some connection between the properties of the Chow variety U of $\mathfrak{U}$ (for instance the non-singularity of U) and the way V is embedded in P^N (or to be more precise, the properties of the linear system of hyperplane sections on V). Our main purpose is to show that, under a mild condition on the embedding of V in P^N, the Chow variety of a maximal, total, regular family is non-singular. As a preparation to this result we first study the Chow varieties of linear systems on V and it turns out that, under the same condition on the embedding of V in P^N, the Chow variety of a linear system is non-singular (Proposition 1).

As we have just mentioned we have to assume some properties for the linear system of hyperplane sections on V in order to be able to prove the non-singularity of U; if these properties are fulfilled, we shall say that V is *adaptable embedded* in P^N (see the definition in Section 2). However, this is not a very serious restriction, for we shall see in Section 2 that the embedding

---

* Received July 25, 1960.

[1] This work was supported at Northwestern University by the National Science Foundation under project NSF-Gg506.

V' of V by means of the hypersurface sections of degree m $(m > 1)$ in P^N always has these properties (Lemma 5). This result can also be interpreted in the following way. If we construct the Chow points by using hypersurfaces of degree m $(m > 1)$ instead of hyperplanes, then the Chow varieties of maximal, total, regular families (and also of linear systems) are non-singular.

In Section 1 we study the degrees of Chow varieties; the Lemmas 1 and 2 are generalizations of results of Chow in [3].

I am very grateful to T. Matsusaka for his valuable help and encouragement during the preparation of this paper.

1. All varieties under consideration are assumed to be projective varieties; therefore the degree of a variety is defined. The ambient projective space of a variety is usually denoted by P^N and $Z_0, Z_1, \cdots, Z_N$ are used as letters for P^N; the ambient projective space of the Chow variety of a system of positive cycles (of a certain dimension and a certain degree) in P^N is usually denoted by P^t, and for P^t we use the letters $Y_0, Y_1, \cdots, Y_t$. If X is a positive cycle in P^N, then its Chow point is denoted by $\mathrm{Ch}(X)$; the degree of a variety V is denoted by $\deg V$.

If P^N is a projective space and if u_{ij} $(j = 0, \cdots, N; i = 1, \cdots, n)$ is a set of elements of the universal domain Ω, then we mean by the linear variety defined by the set of elements (u_{ij}) (or sometimes shortly (u)) the variety defined by the set of equations $\sum_{j=0}^{N} u_{ij} Z_j = 0$ $(i = 1, \cdots, n)$ in P^N.

First, we mention some facts which will be used frequently in the following. Let V^n be a variety in P^N defined over a field k and of degree h. Let $(u_{ij,\sigma})$ $(j = 0, \cdots, N; i = 1, \cdots, n; \sigma = 1, \cdots, r$, where r is some integer) be a system of independent transcendental elements over k, and let L_σ $(\sigma = 1, \cdots, r)$ be the linear variety defined by the set $(u_{ij,\sigma})$ (σ fixed). Then $L_\sigma \cdot V = \sum_{\alpha=1}^{h} Q_{\sigma\alpha}$, where all the $Q_{\sigma\alpha}$ are different from each other. If K_σ denotes the field obtained by adjoining to k all the $(u_{ij,\tau})$ with $\tau \neq \sigma$, then $Q_{\sigma\alpha}$ and $Q_{\sigma\beta}$ $(\beta \neq \alpha)$ are independent generic points of V over K_σ [5, Chap. VIII, Prop. 10]. Therefore, given two arbitrary sets of indices $(\alpha_1, \cdots, \alpha_r)$ and $(\beta_1, \cdots, \beta_r)$ with $1 \leqq \alpha_i, \beta_j \leqq h$, there exists a k-automorphism of the universal domain transforming $Q_{\sigma\alpha_\sigma}$ into $Q_{\sigma\beta_\sigma}$ $(\sigma = 1, \cdots, r)$. Furthermore, let U be the Chow variety of an algebraic system of positive divisors on V. Let H_σ be the hyperplane in the ambient projective space P^t of U defined by the equation $\sum_\rho M_\rho(u_{ij,\sigma}) Y_\rho = 0$ (for some fixed σ), where the $M_\rho(U_{ij})$ range over the monomials of a suitable degree in the U_{ij} (the monomials occurring in the Chow forms of the divisors in the algebraic system associated with U). Such a hyperplane will be called a *hyperplane derived* from the set $(u_{ij,\sigma})$. Then we have by the properties of Chow coordinates (see [1]) for a divisor X in the system that $\mathrm{Ch}(X) \in U \cap H_\sigma$ if and only if X (or better the point set $|X|$) contains some point $Q_{\sigma\alpha}$.

LEMMA 1. *Let V^n be a complete variety, non-singular in codimension* 1 *and of degree h. Let U^r be the Chow variety of an algebraic family $\mathfrak{U}$ of positive divisors on V. Then* $\deg U \geqq h^r$.

Proof. Let k be a field of definition for V and U. Let $(u_{ij,\sigma})$ $(j=0, \cdots, N;\ i=1, \cdots, n;\ \sigma=1, \cdots, r)$ be a set of independent transcendental elements over k. If L_σ $(\sigma=1, \cdots, r)$ is the linear variety in the ambient projective space P^N of V defined by the set $(u_{ij,\sigma})$ and if $L_\sigma \cdot V = \sum_{\alpha=1}^{h} Q_{\sigma\alpha}$, then we can apply to this intersection the remarks preceding the lemma. Let furthermore H_σ $(\sigma=1, \cdots, r)$ be the hyperplanes, in the ambient space P^t of U, derived from the sets $(u_{ij,\sigma})$.

First of all, we want to show that $U \cdot H_1 \cdot \cdots \cdot H_r$ is defined. Clearly, it suffices to show that $U \cdot H_1$ is defined. Let X be a divisor in $\mathfrak{U}$ and algebraic over k. Since every $Q_{1\alpha}$ is generic over k on V, it follows that X contains no point $Q_{1\alpha}$. Therefore (see the remarks preceding the lemma) $\mathrm{Ch}(X) \notin U \cap H_1$, i.e. $U \not\subset H_1$, i.e. $U \cdot H_1$ is defined.

Since $U \cap H_1 \cap \cdots \cap H_r \neq \emptyset$ for dimension reasons and since V is complete and non-singular in codimension 1, it follows that there exists a divisor X in $\mathfrak{U}$ and a set of indices $(\alpha_1, \cdots, \alpha_r)$ such that $Q_{\sigma\alpha_\sigma} \in |X|$ for $\sigma=1, \cdots, r$; let us assume for convenience that $\alpha_\sigma = 1$, i.e. that $Q_{\sigma 1} \in |X|$ for $\sigma=1, \cdots, r$. Given any two set of indices $(\alpha_1, \cdots, \alpha_r)$ and $(\beta_1, \cdots, \beta_r)$, we have seen above that there exists a k-automorphism of the universal domain transforming $Q_{\sigma\alpha_\sigma}$ into $Q_{\sigma\beta_\sigma}$. Since there are precisely h^r such sets, it suffices, in order to prove the lemma, to show that, for some set of indices $(\alpha_1, \cdots, \alpha_r)$, there exists a divisor X^* of $\mathfrak{U}$ such that $Q_{\sigma\alpha_\sigma} \in |X^*|$ for $\sigma=1, \cdots, r$ but $Q_{\sigma\beta} \notin |X^*|$ for all $\beta \neq \alpha_\sigma$ $(\sigma=1, \cdots, r)$. In order to see that, let L_σ' $(\sigma=1, \cdots, r)$ be a linear variety in P^N defined by a set $(u'_{ij,\sigma})$ which is such that:

1. L_σ' goes through $Q_{\sigma 1}$ $(\sigma=1, \cdots, r)$,

2. over the field $K = k(Q_{11}, Q_{21}, \cdots, Q_{r1}, \mathrm{Ch}(X))$ the set (u') is a generic set which fulfills the condition 1.

Since the $Q_{\sigma 1}$ are r independent generic points of V over k, we clearly have over k the generic specialization $(u) \rightarrow (u')$, where (u) stands for the entire set $(\cdots, u_{ij,1}, \cdots; \cdots; \cdots, u_{ij,r}, \cdots)$, and (u') similar. Let $L'_\sigma \cdot V = \sum_{\alpha=1}^{h} Q'_{\sigma\alpha}$

with, say, $Q'_{\sigma 1} = Q_{\sigma 1}$; from the remarks preceding the lemma it follows that $Q'_{\sigma\alpha}$ is a generic point of V over K for $\alpha \neq 1$. Extend the generic specialization $(u) \to (u')$ to a generic specialization $(u', Q', X) \to (u, Q, X^*)$ over k, where the set (Q) contains all the $Q_{\sigma\alpha}$, and (Q') similar. Let under this specialization $Q'_{\sigma 1}$ correspond with $Q_{\sigma\gamma_\sigma}$. Now $Q'_{\sigma 1} \in |X|$, but since $Q'_{\sigma\alpha}$ for $\alpha \neq 1$ is a generic point of V over $K = K(\mathrm{Ch}(X))$, it follows that $Q'_{\sigma\alpha} \notin |X|$ for $\alpha \neq 1$ and $\sigma = 1, \cdots, r$. Therefore it follows that $Q_{\sigma\gamma_\sigma} \in |X^*|$ but $Q_{\sigma\beta} \notin |X^*|$ for $\beta \neq \gamma_\sigma$ $(\sigma = 1, \cdots, r)$. This completes the proof.

LEMMA 2. *Let V^n be a complete variety, non-singular in codimension* 1 *and of degree h. Let U^r be the Chow variety of a linear system $\mathcal{L}$ of divisors on V. Assume that $\mathcal{L}$ is without fixed component. Then* $\deg U = h^r$.

Proof. Let k be a field of definition for V and U and such that the linear system has a module in the function field[1] which has a basis of functions defined over k. We have to consider two different cases.

Case 1. Suppose a generic element of $\mathcal{L}$ has no multiple components. Let L_σ $(\sigma = 1, \cdots, r)$ be the linear varieties in P^N defined by the sets of elements $(u_{ij,\sigma})$ $(j = 0, \cdots, N; 1, \cdots, n)$, where all the $u_{ij,\sigma}$ are transcendental and independent from each other over k. Let $L_\sigma \cdot V = \sum_{\alpha=1}^{h} Q_{\sigma\alpha}$; then we have noted above that $Q_{\sigma\alpha}$ and $Q_{\sigma\beta}$ $(\alpha \neq \beta)$ are two independent generic points of V over the field K_σ (introduced above). Furthermore, for any set of indices $(\alpha_1, \cdots, \alpha_r)$ with $1 \leqq \alpha_\sigma \leqq h$, we have that $Q_{1\alpha_1}, \cdots, Q_{r\alpha_r}$ is a set of r independent generic points of V over k, and therefore there is precisely one element X in the linear system going through $Q_{1\alpha_1}, \cdots, Q_{r\alpha_r}$. If we denote this X by $X_{\alpha_1 \cdots \alpha_r}$, then $X_{\alpha_1 \cdots \alpha_r}$ is rational over the field $K_{\alpha_1 \cdots \alpha_r} = k(Q_{1\alpha_1}, \cdots, Q_{r\alpha_r})$. Since, as we have seen above, $Q_{\sigma\beta}$ for $\beta \neq \alpha_\sigma$ is a generic point of V over this field, it follows that $X_{\alpha_1 \cdots \alpha_r}$ does not contain $Q_{\sigma\beta}$. Therefore $X_{\alpha_1 \cdots \alpha_r} \neq X_{\beta_1 \cdots \beta_r}$ if for some σ the $\alpha_\sigma \neq \beta_\sigma$.

Next, let H_σ $(\sigma = 1, \cdots, r)$ be the hyperplane in the ambient projective space of U derived from the set $(u_{ij,\sigma})$. Then we have, according to the remarks made above, that $\mathrm{Ch}(X_{\alpha_1 \cdots \alpha_r}) \in U \cap H_1 \cap \cdots \cap H_r$ for every set of indices $(\alpha_1, \cdots, \alpha_r)$ and moreover these are the only points in this intersection. Since we obtain in this way precisely h^r (different) points, it suffices, in order to complete the proof, to see that every point has multiplicity 1 in this intersection. From the fact that $X_{\alpha_1 \cdots \alpha_r}$ contains the points $Q_{1\alpha_1}, \cdots, Q_{r\alpha_r}$, which are r independent generic points of V over k, it follows easily that the point $\mathrm{Ch}(X_{\alpha_1 \cdots \alpha_r})$ is generic on U over k; therefore it is in particular simple. Since (as is easily seen) the $X_{\alpha_1 \cdots \alpha_r}$ are conjugate to each other over the field obtained by adjoining the coefficients $u_{ij,\sigma}$ of the L_σ to the ground field k, it suffices to consider only one of the $X_{\alpha_1 \cdots \alpha_r}$, and let us write X instead of $X_{\alpha_1 \cdots \alpha_r}$. We have to show that $H_1 \cdot \cdots \cdot H_r$ is transversal to the tangent space to U at $\mathrm{Ch}(X)$. Since the $H_1, \cdots, H_r$ are r independent generic derived hyperplanes over the ground field k, it suffices to show that there are some r derived hyperplanes $H'_1, \cdots, H'_r$ such that $H'_1 \cdot \cdots \cdot H'_r$ is defined and transversal with the tangent space to U at $\mathrm{Ch}(X)$ (for then over the specialization $H_i \to H'_i$ over k there is an $X_{\beta_1 \cdots \beta_r}$ specializing to X and hence $H_1 \cdot \cdots \cdot H_r$ is transversal to the tangent space to U at $\mathrm{Ch}(X_{\beta_1 \cdots \beta_r})$, which is sufficient since $X_{\alpha_1 \cdots \alpha_r}$ and $X_{\beta_1 \cdots \beta_r}$ are conjugate). However, now we contend that the intersection of all the derived hyperplanes through $\mathrm{Ch}(X)$ is $\mathrm{Ch}(X)$ itself, which is clearly sufficient for the existence of r derived hyperplanes $H'_1, \cdots, H'_r$ with the above mentioned property. In order to see that the contention is true let $\mathrm{Ch}(X) = (c_\lambda)$ and let (d_λ) be an arbitrary point in the ambient space P^t of U. Consider the Chow form $\sum c_\lambda M_\lambda(U) = F(U)$ and the form $\sum d_\lambda M_\lambda(U) = G(U)$. We must try to find a set (u') such that $F(u') = 0$ and $G(u') \neq 0$. However, if $(c_\lambda) \neq (d_\lambda)$, then the existence of such a set (u') follows from the fact that $F(U)$ has no multiple factors since X has no multiple components.

---

[1] Let $\mathcal{L}$ be a linear system on V; let Ω be the universal domain and $\Omega(V)$ the function field of V. We shall say that a vector space $M \subset \Omega(V)$ over Ω is a module for $\mathcal{L}$ if there exists a (fixed) divisor Y on V such that $(f) + Y \in \mathcal{L}$ for all functions $f \in M$ and if conversely for every $X \in \mathcal{L}$ there exists an $f \in M$ such that $X = (f) + Y$. Such a module always exists; in particular, if we take an $X_0 \in \mathcal{L}$, then the set $L(X_0) = \{f \mid f \in \Omega(V)$ such that $(f) = X - X_0$ with $X \in \mathcal{L}\}$ is a module for $\mathcal{L}$.

Case 2. Suppose a generic member X (over k) of $\mathcal{L}$ has multiple components. According to [9, Th. 1. 6. 3] we have $X = p^e X'$, where X' has no multiple components and p is the characteristic of the universal domain. In order not to interrupt the arguments later on we first state an auxiliary lemma.

LEMMA 3. *Let U be a projective variety defined over a field k of characteristic p and let P be a generic point of U over k. Let U^* be the locus of $P^{(p^e)}$ over the field $k^{(p^e)}$, where $P^{(p^e)}$ is the point obtained by raising the coordinates of P to the p^e-th power. Then* $\deg U = \deg U^*$.

For the proof of Lemma 3 it suffices to remark that we obtain U^* from U by applying the Frobenius automorphism $\rho \to \rho^{p^e}$ to the universal domain and that by this automorphism hyperplanes go over in hyperplanes.

Returning to the proof of Case 2 of Lemma 2, take a fixed divisor X_0 in $\mathcal{L}$ and let k be an algebraically closed field over which V and U are defined, over which X_0 is rational and such that the function module $L(X_0)$ of $\mathcal{L}$ has a base of functions defined over k. Let X be a generic member of $\mathcal{L}$ over k; then we have $X = p^e X'$ as we have seen above. Let U' be the locus of the

$\mathrm{Ch}(X')$ over k. If $\mathrm{Ch}(Y') \in U'$, then $\mathrm{Ch}(p^e Y') \in U$, and conversely if $\mathrm{Ch}(Y) \in U$, then $Y = p^e Y'$ with a Y' such that $\mathrm{Ch}(Y') \in U'$; in particular $X_0 = p^e X_0'$ with $\mathrm{Ch}(X_0') \in U'$. By [9, Prop. 1.6.4] we have $L(X_0) \subset (\Omega(V))^{(p^e)}$, where Ω is the universal domain and $\Omega(V)$ is the function field of V over Ω. If $\mathrm{Ch}(Y') \in U'$, then $p^e Y' = X_0 + (f)$ with $f \in L(X_0)$ and hence $Y' - X_0' = (f^{1/p^e})$ with $f^{1/p^e} \in \Omega(V)$, and hence $Y' \sim X_0'$. Moreover, it is then easily seen that U' is the Chow variety of a linear system $\mathcal{L}'$ without fixed components, a generic element X' of which has no multiple components. Let $P^{t'}$ be the ambient space of U'. Let $(c_\lambda) = \mathrm{Ch}(X')$ and $(d_\mu) = \mathrm{Ch}(X)$; then we can rearrange the coordinates d_μ such that $d_\nu = c_\nu^{p^e}$ for $\nu = 1, \cdots, t'$ and $d_\nu = 0$ for $\nu = t' + 1, \cdots, t$. Therefore there is a projection of the ambient space P^t of U onto $P^{t'}$ such that the image of U is the variety U^*, where U^* is the locus of $(\mathrm{Ch}(X'))^{(p^e)}$ over k and clearly $\deg U = \deg U^*$. By Lemma 3 $\deg U^* = \deg U'$ and $\deg U' = h^r$ by Case 1, which completes the proof.

2. Let V^n be a complete, projective variety defined over k.

LEMMA 4. *Let $\mathcal{L}$ be a linear system of divisors on V having the following properties:*

1. *If P, P' are any two simple points on V, then the linear subsystem $\mathcal{L}(P,P')$ of $\mathcal{L}$, consisting of all divisors of $\mathcal{L}$ going through P and P', has no base points (except P and P').*

2. *If $K \supset k$ is any field such that $\mathcal{L}$ has an associated function module with a basis of functions defined over K and if $Y_1, \cdots, Y_n$ are n independent generic members of $\mathcal{L}(P,P')$ over $K(P,P')$, then $Y_1 \cdot \cdots \cdot Y_n$ is defined and equal to $1 \cdot P + 1 \cdot P' + W$, where W is a cycle not containing P and P'.*

Under these assumptions, if $X_1, \cdots, X_n$ are n independent generic members of $\mathcal{L}(P)$ over $K(P)$, then:

a. *$X_1 \cdot \cdots \cdot X_n$ is defined and equal to $1 \cdot P + 1 \cdot Q_1 + \cdots + 1 \cdot Q_a$,*

b. *if $i \neq j$, then Q_i and Q_j are independent generic points of V over $K(P)$.*

Proof. First, we remark that if A is a subvariety of V algebraic over $K(P)$ and different from V itself, then $X_1 \cap \cdots \cap X_n \cap A = \emptyset$. For it follows from 1. that $\mathcal{L}(P)$ has no fixed points and therefore a generic X_1 does not contain A, and it follows that the dimension of every component of $X_1 \cap A$ is smaller than the dimension of A. By repeating the argument we see that $X_1 \cap X_2 \cap \cdots \cap X_n \cap A = \emptyset$. Now let $Q \in X_1 \cap \cdots \cap X_n$ $(Q \neq P)$; then it follows from the above remark that Q is a simple point on V. Next, let $Y_1, \cdots, Y_n$ be as in 2. for $\mathcal{L}(P, Q)$; we have $(X_1, \cdots, X_n) \to (Y_1, \cdots, Y_n)$ over $K(P)$. Therefore $X_1 \cdot \cdots \cdot X_n$ is defined, and P and at least one other point in $X_1\cdot\cdots\cdot X_n$ have multiplicity 1. Put $K_1 = K(P)$; let $\phi_1,\cdots,\phi_N$ be a base for a function module of $\mathcal{L}(P)$ such that all ϕ_i are defined over K_1; moreover, we can assume that all ϕ_i are defined at Q and that at least one ϕ_i, say ϕ_1, is such that $\phi_1(Q)\neq 0$ (since Q is no base point for $\mathcal{L}(P)$). Let $X_i = (\sum_{\rho=1}^{N} u_{i\rho}\phi_\rho)_0$, $i=1,\cdots,n$, with the $u_{i\rho}$ independent transcendentals over K_1. We have $\dim_{K_1} K_1(u,Q) = \dim_{K_1} K_1(u) = Nn$. Since

$$u_{i1}\in K_1(Q, u_{i2},\cdots,u_{iN}) \text{ for } i=1,\cdots,n,$$

we see that $\dim_{K_1(Q)} K_1(Q,u) \leqq (N-1)n$. Then it follows from the tower $K_1 \subset K_1(Q) \subset K_1(Q,u)$ that

$$\dim_{K_1} K_1(Q) = n \text{ and } \dim_{K_1(Q)} K_1(Q,u) = (N-1)n.$$

Then $X_1,\cdots,X_n$ are n independent generic members of $\mathcal{L}(P,Q)$ over $K(P,Q)$; for, the dimension of $\mathcal{L}(P)$ being N and Q being not a fixed point of $\mathcal{L}(P)$, the dimension of $\mathcal{L}(P,Q)$ is $N-1$. Then a. follows from 2. applied to $\mathcal{L}(P,Q)$. Now let Q_i and Q_j be as in b. From what we just have seen it follows that $X_1,\cdots,X_n$ are n independent members of $\mathcal{L}(P,Q_i)$ over $K(P,Q_i)$. If the locus of Q_j over this field has a dimension smaller than n, then, since $\mathcal{L}(P,Q_i)$ has by assumption no base points (except P and Q_i), it follows by the same argument as in the beginning of this proof that $X_1\cap\cdots\cap X_n$ has an empty intersection with every component of the locus of Q_j. This being a contradiction, it follows that Q_j has dimension n over $K(P,Q_i)$.

LEMMA 5. *The linear system $\mathcal{L}_m$ $(m>1)$ of hypersurface sections of degree m on V is ample and has the properties* 1. *and* 2. *of Lemma* 4.

Proof. It is well known that $\mathcal{L}_m$ is ample. Given P and $P'\in V$ and an arbitrary point Q in the ambient projective space P^N of V, then there clearly exists a hypersurface of degree m (if $m>1$) through P and P' but not through Q. As to property 2., let $H_m^{(i)} = L^{(i)} + H_{m-1}^{(i)}$, $(i=1,\cdots,n)$, where $L^{(i)}$ is a hyperplane through P and $H_{m-1}^{(i)}$ is a hypersurface of degree $m-1$ through P', and moreover we take generic $L^{(i)}$ and $H_{m-1}^{(i)}$ with these properties and all independent from each other (over a field $K(P,P')$ as in Lemma 4). Since in particular $L^{(i)}$ does not go through P' and $H^{(i)}$ not through P, we have if we put $V\cdot H_m^{(i)} = X_i'$ that $X_1'\cdot\cdots\cdot X_n'$ has property 2 in Lemma 4, so certainly for generic X_i we have this property.

Definition. A variety V^n is *adaptable embedded* in projective space P^N if $V\subset P^N$ and if this embedding has the following property. If k is a field of definition for V and P a simple point on V rational over k, and if L^{N-n} is a linear variety through P but otherwise generic over k, then:

1. $V \cdot L = P + \sum_{i=2}^{h} Q_i$ with $Q_i \neq Q_j$ for $i \neq j$ $(h = \deg V)$,

2. for every pair (i, j) with $i \neq j$, the points Q_i and Q_j are independent generic points of V over k.

LEMMA 6. *Let V^n be a variety in projective space P^N. Let V' be the embedding of V into projective space P^M by means of the hypersurface sections of degree m $(m > 1)$. Then V' is adaptable embedded in P^M.*

Proof. Instead of considering $V' \cdot L$ in P^M we can consider in P^N the intersection $V \cdot H$, where H is a complete intersection of n hypersurfaces of degree m, independent generic from each other over the field k in consideration (except for going through the given point P). The lemma follows then from Lemma 5 and Lemma 4.

3. LEMMA 7. *Let U be the Chow variety of an algebraic system of positive r-dimensional cycles in P^N, defined over a field k with a generic element X over k. Let Z be a k-rational positive r-dim. cycle. Let W be the locus of $\mathrm{Ch}(X + Z)$ over k. Then there is an everywhere biregular birational transformation between U and W.*

Proof. Let U be in P^t. Let $\sum_{\lambda=0}^{t} \xi_\lambda M_\lambda(U)$ be the Chow form of X and let $F(U) = \sum \xi_\lambda{}^* M_\lambda(U)$ be a form with generic $(\xi_\lambda{}^*)$ over k. Suppose $\sum \alpha_\nu N_\nu(U) = G(U)$ is the Chow form of Z. Put $F(U) \cdot G(U) = H(U) = \sum_{\mu=0}^{s} \eta_\mu L_\mu(U)$. Then W is in P^s. Furthermore, $\eta_\mu = \rho_\mu(\xi^*)$, where the ρ_μ are linear forms in the ξ^*. These forms define a projective transformation of P^t into P^s; since it follows clearly, from the way the η_μ are defined, that there is no (ξ') such that all $\rho_\mu(\xi')$ are zero, it follows that P^t is transformed in a one-to-one manner to a subspace of P^s. W is then clearly the projective transformation of U.[2]

PROPOSITION 1. *Let V be a complete variety, non-singular in codimension 1 and adaptable embedded in projective space. The the Chow variety of a linear system is non-singular.*

Proof. Let U^r be the Chow variety of a linear system $\mathscr{L}$; let $\deg V^n = h$. By Lemma 7 we can assume that $\mathscr{L}$ has no fixed components. Let $X \in \mathscr{L}$; since $\mathscr{L}$ has no fixed components, there is a point $P \in |X|$ which is not a base point for $\mathscr{L}$; we can assume that P is simple on V. Let k be a field of definition for V and U, such that X and P are rational over k and such that $\mathscr{L}$ has a function module with a basis of functions defined over k. Let L^{N-n}

---

[2] It follows from this that the assumption in Lemma 2 that $\mathscr{L}$ has no fixed components can be omitted.

be a linear variety in the ambient space P^N of V, going through P but otherwise generic over k defined by a set of elements (u_{ij}) $(j=0,\cdots,N;$ $i=1,\cdots,n)$. Let $V\cdot L = P + \sum_{i=2}^{h} Q_i$ (by assumption on the embedding $Q_i \neq Q_j \neq P$). Let H be the hyperplane in the ambient space P^t of U derived from the set (u_{ij}); $U \cap H$ consists of all divisors in $\mathcal{L}$ which contain at least one point of $V \cap L$. Denote by $\mathcal{L}_P$, resp. $\mathcal{L}_{Q_i}$ $(i=2,\cdots,h)$, the linear subsystems of $\mathcal{L}$ consisting of all divisors through P, resp. Q_i. $\mathcal{L}_P$ is a proper subsystem of $\mathcal{L}$ (since P is not a base point) and also the $\mathcal{L}_{Q_i}$ are proper; in fact, $X \notin \mathcal{L}_{Q_i}$ since Q_i is generic on V over k and X is rational over k. Moreover, for $i \neq j$ we have $\mathcal{L}_{Q_i} \neq \mathcal{L}_{Q_j}$ since Q_i and Q_j are independent generic points of V over k (since V is adaptable embedded). Let U_P, U_i $(i=2,\cdots,h)$ be the Chow varieties of $\mathcal{L}_P$ and $\mathcal{L}_{Q_i}$ respectively. Then the above stated properties can be translated as follows

$$U \cap H = U_P \cup U_2 \cup \cdots \cup U_h, \quad \mathrm{Ch}(X) \notin U_i \quad (i=2,\cdots,h)$$

and $U_i \neq U_j$ for $i \neq j$. By Lemma 2 $\deg U = h^r$; by Lemma 1 $\deg U_P \geqq h^{r-1}$ and $\deg U_i \geqq h^{r-1}$ $(i=2,\cdots,h)$. Therefore we most have

$$U\cdot H = 1\cdot U_P + \sum_{i=2}^{h} 1\cdot U_i.$$

By the criterion of multiplicity 1 [8; VI, Th. 6] the proposition is proved if $\dim U = 1$, and if $\dim U > 1$, it suffices to prove (since $\mathrm{Ch}(X) \notin U_i$) that $\mathrm{Ch}(X)$ is simple on U_P. Therefore proceeding by induction on $\dim U$ the proof is complete.

PROPOSITION 2.[3] *Let V^n be a complete, non-singular projective variety. Let U be the Chow variety of a maximal, total, regular family $\mathcal{U}$ of positive divisors on V. Let $X \in \mathcal{U}$; then the Chow variety of the complete linear system $\mathcal{L}(X)$, determined by X, is a simple subvariety of U.*

Proof. Let $\mathrm{Ch}(X_0)$ be a simple point of U and let k be a common field of definition for V, U and the Pic.(V) over which X and X_0 are rational. Consider the rational mapping $h\colon U \to \mathrm{Pic.}(V)$ defined by $h(\mathrm{Ch}(X^*)) = \mathrm{Class}(X^* - X_0)$, where X^* is a generic element of $\mathcal{U}$ over k; h is defined over k. Let Γ_h be the graph of h on $U \times \mathrm{Pic.}(V)$. Let $\mathrm{Ch}(X^*)$ be a generic point of U over k, put $\eta^* = \mathrm{Cl.}(X^* - X_0)$ and $\eta = \mathrm{Cl.}(X - X_0)$. If we denote by $\mathcal{L}(X^*)$, resp. $\mathcal{L}(X)$, also the Chow varieties of the complete linear systems determined by X^*, resp. X, then we have by [6, I, Prop. 10 and Cor.] $\Gamma_h\cdot(P^t \times \eta^*) = \mathcal{L}(X^*) \times \eta^*$ and $\Gamma_h \cap (P^t \times \eta) = \mathcal{L}(X) \times \eta$. Since $\mathcal{U}$ is a regular family, all the linear systems have the same dimension, and then it follows by Lemma 2 (and footnote 2) that the corresponding Chow varieties have the same degree. Therefore we must have $\Gamma_h \cdot (P^t \times \eta) = \mathcal{L}(X) \times \eta$ (and not a multiple of that cycle since this contradicts the fact that $\Gamma_h \cdot (P^t \times \eta)$ is the specialization of $\Gamma_h \cdot (P^t \times \eta^*)$ over the specialization $\eta^* \to \eta$ with respect to k). Hence by the criterion of multiplicity 1 [8, VI, Th. 6] we see that $\mathcal{L}(X) \times \eta$ is a simple subvariety of Γ_h. It suffices therefore to show that the mapping h is regular (in the sense of [8]) at the subvariety $\mathcal{L}(X)$ of U.

---

[3] The writer owes this proposition to T. Matsusaka; it is of special interest for it follows from this proposition that the Picard variety can be constructed in precisely the same way as the Jacobian variety is constructed by Chow in [3]. (See the remark following this proposition.)

Let C be a generic 1-section of V over k, J the Jacobian of C and $\phi \colon C \to J$ the canonical mapping. Let B be the abelian subvariety of J generated by the points $S\phi((X^* - X_0) \cdot C)$. Then by [4] [4] B is a model for the Pic.(V) and the mapping $h' \colon U \to B$ defined by $h'(\mathrm{Ch}(X^*)) = S\phi((X^* - X_0) \cdot C)$ is the canonical mapping; hence we can take Pic.$(V) = B$ and $h = h'$. If $K \supset k$ is such that C, J, ϕ are defined over K, then we must show that h' is regular at $\mathrm{Ch}(X')$, where $\mathrm{Ch}(X')$ is a generic point of $\mathcal{L}(X)$ over K. In view of its application in the next theorem we state the next lemma.

LEMMA 8. *If C is a generic* 1*-section of V over $k(\mathrm{Ch}(X'))$ and if J, ϕ, B and h' are introduced as above, then h' is regular at* $\mathrm{Ch}(X')$.

Proof. Instead of considering h' we can consider $f \colon U \to J$ defined by $f(\mathrm{Ch}(X^*)) = S\phi(X^* \cdot C)$ since h' and f differ only by a constant on J. Let $\deg(X^* \cdot C)$ be d. Then we have the following commutative diagram:

$$\begin{tikzcd}
U \arrow[rr, "f"] \arrow[dr, "g"'] & & J \\
& C^{(d)} \arrow[ur, "\psi"'] &
\end{tikzcd}$$

---

[4] Since [4] is still unpublished, we indicate how the proof here can also be obtained from Chow's results. It is irrelevant for our considerations that Pic.(V) is embedded in one Jacobian, an embedding into a product of Jacobians is sufficient. By the so-called regularity theorem [Lang, Abelian Varieties, VIII, Th. 9] there is such an embedding. However, we must also have a connection between the natural mapping $X \to \mathrm{Cl.}(X - X_0)$ and the intersection of X with the generic 1-sections. In fact, we must have commutativity in the following diagram (where we can restrict to one Jacobian),

$$\begin{tikzcd}
U \arrow[rr, "\psi"] \arrow[dr, "h"'] & & J_u \\
& \mathrm{Pic.}(V) \arrow[ur, "\lambda_u"'] &
\end{tikzcd}$$

where h is the natural mapping $X \to \mathrm{Cl.}(X - X_0)$, λ_u is the canonical mapping of the $k(u)/k$-trace Pic.(V) to J_u and $\psi(Ch(X)) = S\phi((X - X_0) \cdot C_u)$. This commutativity follows essentially from Th. 12 and Th. 4 in Lang's book, Chap. VIII.

where $C^{(d)}$ is the Chow variety of positive divisors of degree d on C, g is the mapping $g(\mathrm{Ch}(X^*)) = \mathrm{Ch}(X^*\cdot C)$ and ψ is the mapping $\psi(\sum_{j=1}^{d} P_j) = S\phi(P_j)$, where P_j are points on C. Since $C^{(d)}$ is non-singular,[5] it suffices to prove that g is regular at $\mathrm{Ch}(X')$. Let the Chow form of X' be $\sum_\lambda \xi_\lambda M_\lambda(U)$ where the $M_\lambda(U)$ are monomials in the letters U_{ij} $(j = 0, \cdots, N;\ i = 1, \cdots, n)$. Let C be the intersection of V with a linear space L defined by $\sum_{j=0}^{N} v_{ij}Z_j = 0$ $(i = 1, \cdots, n-1)$ with v_{ij} independent transcendentals over $k(\mathrm{Ch}(X'))$. Putting $L\cdot X' = \sum_{\alpha=1}^{d} P_\alpha$ with $P_\alpha = (p_{\alpha 0}, \cdots, p_{\alpha N})$ we have by the definitions of the Chow forms of X' and $X'\cdot L$ the relation

$$\sum \xi_\lambda M_\lambda(v, \cdots U_{nj} \cdots) = \rho(v)\prod_{\alpha=1}^{d}\Big(\sum_{j=0}^{N} U_{nj}p_{\alpha j}\Big) = \rho(v)\sum_\mu \eta_\mu N_\mu(U),$$

where $\rho(v)$ is a rational function in the v's and $\sum_\mu \eta_\mu N_\mu(U)$ is the Chow form of $X'\cdot L$ (in the letters U_{nj}). Therefore the η_μ are polynomials in the ξ_λ (with coefficients in $k(v)$) and since, of course, not all these polynomials are zero, the mapping g is regular at $\mathrm{Ch}(X')$.

Remark. It follows from Proposition 2 that the variety W of [6, II, page 59] is itself a model for the Pic. (V). It follows from the properties stated there that is suffices, in order to show this, that W is non-singular. W is the Chow variety of the family of linear systems $\mathscr{L}(X)$ on U. Since $\mathfrak{U}$ is regular, every linear system has the same dimension and therefore by Lemma 2 the same degree. Therefore we have an involutional system in the sense of [2]. By a theorem of Chow [2, p. 258] it suffices to show that each $\mathscr{L}(X)$ is a simple subvariety of U, but this is precisely the assertion of Proposition 2.[6]

THEOREM. *Let V be a complete, non-singular variety, adaptable embedded in projective space. Then the Chow variety of a maximal, total, regular family of positive divisors on V is non-singular.*

Proof. Let U be the Chow variety under consideration; let $\mathrm{Ch}(X) \in U$. Let $\mathrm{Ch}(X_0)$ be a simple point on U. Consider as in the proof of Proposition 2 the mapping $h\colon U \rightarrow \mathrm{Pic.}(V)$ defined by $h(\mathrm{Ch}(X^*)) = \mathrm{Cl.}(X^* - X_0)$, where $\mathrm{Ch}(X^*)$ is a generic point of U (over a field k of definition for V and U over which X and X_0 are rational). Let $\eta = \mathrm{Cl.}(X - X_0)$; then, if Γ_h is the graph of h, we have seen that $\Gamma_h \cdot (P^t \times \eta) = \mathcal{L}(X) \times \eta$ (P^t is, as usual, the ambient space of U, $\mathcal{L}(X)$ is the Chow variety of the linear system determined by X). First, we want to show that $\mathrm{Ch}(X) \times \eta$ is simple on Γ_h. By [8, VI, Th. 6] it suffices to show that $\mathrm{Ch}(X) \times \eta$ is simple on $\mathcal{L}(X) \times \eta$. This follows from the fact that $\mathcal{L}(X)$ is non-singular by Proposition 1. Therefore it suffices to show that h is regular at $\mathrm{Ch}(X)$. Introducing a generic 1-section C of V over k and J and B and h' as above we can take by [4] $\mathrm{Pic.}\,V = B$ and $h = h'$. Then h' is regular at $\mathrm{Ch}(X)$ by Lemma 8.

---

[5] There is an oversight on page 472 of [3] in the proof of the non-singularity of $C^{(d)}$ (in case the divisor has multiple components). However, by using the same arguments as in the proof of Proposition 1 this can be corrected; the essential point being that we know the degree of the Chow variety $C^{(d)}$ in terms of the degree of C.

[6] The method of Matsusaka for constructing the Picard variety can also be used to construct the so-called "generalized Picard varieties" in the sense of Tate (see L. Lang, Abelian Varieties, page 176). We hope to return to this question on some future occasion.

NORTHWESTERN UNIVERSITY AND
STATE UNIVERSITY, LEIDEN (NETHERLANDS).

REFERENCES.

[1] W. L. Chow and B. L. van der Waerden, "Zur algebraischen Geometrie IX," *Mathematische Annalen*, vol. 113 (1937), pp. 692-704.

[2] W. L. Chow, "Algebraic systems of positive cycles in an algebraic variety," *American Journal of Mathematics*, vol. 72 (1950), pp. 247-283.

[3] ———, "The Jacobian variety of an algebraic curve," *ibid.*, vol. 76 (1954), pp. 453-476.

[4] W. L. Hoyt, Unpublished (to appear soon).

[5] S. Lang, *Introduction to Algebraic Geometry*, Interscience, New York, 1958.

[6] T. Matsusaka, "On the algebraic construction of the Picard variety I and II," *Japanese Journal of Mathematics*, vol. XXI (1951), and vol. XXII (1952), pp. 217-235 resp. pp. 51-62.

[7] ———, "On algebraic families of positive divisors and their associated varieties," *Journal of the Mathematical Society of Japan*, vol. 5 (1953), pp. 113-136.

[8] A. Weil, *Foundations of Algebraic Geometry*, American Mathematical Society Colloquium Publications, vol. 24, New York, 1946.

[9] O. Zariski, *Introduction to the problem of minimal models in the theory of algebraic surfaces*, Publications of the Mathematical Society of Japan, vol. 4 (1958).

ON THE ALGEBRA OF REPRESENTATIVE FUNCTIONS OF AN ANALYTIC GROUP.*

By G. Hochschild and G. D. Mostow.

1. Introduction. Let G be a real or complex analytic group. If ρ is an analytic finite dimensional representation of G, and if t is a linear functional on the algebra of all linear endomorphisms of the representation space of ρ, then the composite $t \circ \rho$ is called a representative function on G associated with ρ. Throughout, R, or $R(G)$, if the group is to be exhibited, denotes the algebra of all complex valued representative functions on G. In the analysis of R, a special role is played by the group $\mathrm{Hom}(G, C)$ of all analytic homomorphisms of G into the additive group C of the complex numbers. By composition with the exponential map of C into the multiplicative group C^* of the non-zero complex numbers, we obtain the subgroup $Q = \exp(\mathrm{Hom}(G, C))$ of the group $\mathrm{Hom}(G, C^*)$ of all analytic homomorphisms of G into C^*. It is a fundamental feature of the generalized Tannaka Theorem (see [2], [3], [4]) that the departure of the representation theory of G from that of an algebraic linear group depends entirely on the non-triviality of Q. It is for this reason that Q is singled out in a natural way in the structure of R.

A subalgebra B of R will be called a *basic subalgebra* if it satisfies the following conditions: (1) B contains the constants, (2) $B[Q] = R$, (3) the elements of Q are free over B, (4) in the real case, B is stable under the complex conjugation of R. It is known from [3] and [4] that *there always exists a finitely generated basic subalgebra.* However, this result is inadequate in as much as it ignores the G-module structure of R. Actually, we shall show in Section 3 that there always exists a basic subalgebra that is stable under the left G-translations and, in fact, has the additional stability property that its 'semisimple part' is stable under both the left and the right G-translations. Although it is easy to see (Section 3) that all basic subalgebras are isomorphic as algebras, they may differ radically in their behaviour under the action of G. On the other hand, we shall show in Section 4 that the *normal basic subalgebras,* i. e., the basic algebras that are left stable and whose semisimple part is two-sidedly stable, can be classified into orbits under the right G-translations, which correspond in a natural 1-1 fashion to the con-

---

* Received August 10, 1960.

jugacy classes of the decompositions of G into semidirect products of the type described in Section 2.

In Section 6, we analyze the group of the proper automorphisms of R (i. e., the automorphisms leaving the constants fixed and commuting with the right translations) by means of a stable basic subalgebra. In particular, we show that this group is a semidirect product of a subgroup naturally isomorphic with $\mathrm{Hom}(Q, C^*)$ by the normal subgroup of the left translations (complexified, in the real case). Section 7 is a direct application of the existence of stable basic subalgebras and concerns the representations of G as *closed* subgroups of full linear groups.

In Section 8, we show that the *two-sidedly stable* basic subalgebras (which do not always exist) correspond in a 1-1 fashion to the rational equivalence classes of faithful representations of the *complex* analytic group G as an algebraic linear group. In particular, it follows from this and the correspondence between normal basic subalgebras and decompositions of G that any two such 'algebraic structures' of G are conjugate by an analytic automorphism of G, whence we obtain a description of the set of all algebraic structures on G which exhibits this set as an affine space in a natural way. On the level of the decomposition theory of G, the conjugacy result is due to B. Kostant (Theorem 8. 4).

The statements of the results obtained here and the main features of their proofs are intelligible without reference to our previous papers ([2], [3], [4]) on this topic. Nevertheless, we lean heavily on the notions and techniques of these papers, and we have not covered all the details of the proofs by explicit references.

2. Nuclei and decompositions.

For later use, we review some known results concerning decompositions of analytic groups into semidirect products.

We shall say that a (real or complex) Lie group G is *reductive* if G has a faithful finite dimensional analytic representation and if every finite dimensional analytic representation of G is semisimple. By a *nucleus* of a Lie group G we shall mean a closed, normal, solvable and simply connected analytic subgroup K of G such that G/K is reductive. Let N denote the radical of the commutator subgroup G' of G. Then every finite dimensional analytic representation of G is unipotent on N. Now suppose that G has a nucleus K. Then G has a finite dimensional semisimple analytic representation whose kernel is exactly K. Since the restriction of a semisimple representation to a normal subgroup is still semisimple, we conclude that $N \subset K$. Thus N *is contained in every nucleus of* G.

If G is an analytic group that has a faithful finite dimensional analytic representation then G has a nucleus. Moreover, if K is any nucleus of G then G is a semidirect product $H \cdot K$, where H is a closed analytic subgroup of G and, of course, is reductive.

In the complex case, the existence of a nucleus K for an analytic group G implies the existence of a semidirect product decomposition $G = H \cdot K$, even when it is not assumed that G is faithfully representable, and the existence of a faithful representation is then a consequence of the existence of a nucleus [4, Th. 3.6]. In the real case, the proof of the second assertion above is contained in the proof of [2, Th. 9.1]; one merely has to observe that any given nucleus of G may take the place of the group K used in that proof. The first of our two assertions above, in the real case, is part of [2, Th. 9.1]; in the complex case, the existence of a nucleus is part of [4, Th. 4.2].

In our later applications of nuclei, we shall use the fact that the Lie algebra of K can be written as a sum of the Lie algebra of N and another nilpotent Lie algebra that lies in the centralizer of the Lie algebra of H. What we shall need is contained in the following lemma.

LEMMA 2.1. *Let $\mathfrak{G}$ be a Lie algebra that is a semidirect sum $\mathfrak{H} + \mathfrak{K}$, where $\mathfrak{K}$ is a solvable ideal and $\mathfrak{H}$ is a complementary subalgebra that is reductive in $\mathfrak{G}$. Let $\mathfrak{N} = [\mathfrak{G}, \mathfrak{K}]$. Then there is a nilpotent subalgebra $\mathfrak{P}$ of $\mathfrak{K}$ such that $[\mathfrak{H}, \mathfrak{P}] = (0)$ and $\mathfrak{K} = \mathfrak{P} + \mathfrak{N}$ (not necessarily semidirect).*

Proof. Let $\mathfrak{L}$ denote the centralizer of $\mathfrak{H}$ in $\mathfrak{K}$. Since $\mathfrak{K}$ is semisimple as an $\mathfrak{H}$-module (under the adjoint representation), it is clear that $\mathfrak{K} = \mathfrak{L} + \mathfrak{N}$. For $x \in \mathfrak{L}$, denote by $\mathfrak{L}^x$ the subspace of all elements of $\mathfrak{L}$ that are annihilated by some power of the inner derivation effected by x. If we choose x so that $\mathfrak{L}^x$ is of the smallest possible dimension then $\mathfrak{L}^x$ (is a Cartan subalgebra of $\mathfrak{L}$ and, in particular,) is a nilpotent subalgebra $\mathfrak{P}$ of $\mathfrak{L}$. By Fitting's Lemma, we have $\mathfrak{L} = \mathfrak{P} + \mathfrak{S}$, where $\mathfrak{S}$ is a subspace such that $[x, \mathfrak{S}] = \mathfrak{S}$. Hence $\mathfrak{S} \subset \mathfrak{N}$, and we conclude that $\mathfrak{K} = \mathfrak{P} + \mathfrak{N}$, completing the proof.

3. **Basic subalgebras.**

We begin with two elementary facts concerning basic subalgebras that are important for our purpose.

PROPOSITION 3.1. *Let U and V be any two basic subalgebras of R. Then there exists a unitary C-algebra isomorphism of U onto V.*

Proof. For every $f \in R$, write $f = \sum_{q \in Q} v_q(f) q$, with $v_q(f) \in V$. Similarly, define the maps $u_q \colon R \to U$, for each $q \in Q$. Now define the map $\phi \colon U \to V$ by $\phi(f) = \sum_{q \in Q} v_q(f)$. Then ϕ is evidently a unitary C-algebra homomorphism of U into V. Interchanging the roles of U and V, we obtain a unitary C-algebra homomorphism $\psi\colon V \to U$. Let $f \in U$. Then we have

$$\begin{aligned}\psi(\phi(f)) &= \textstyle\sum_q u_q(\phi(f)) = \sum_{q,q'} u_q(v_{q'}(f))\\ &= \textstyle\sum_{q,q'} u_{qq'}(v_{q'}(f)q')\\ &= \textstyle\sum_q u_q(\sum_{q'} v_{q'}(f)q')\\ &= \textstyle\sum_q u_q(f) = f.\end{aligned}$$

Thus $\psi \circ \phi$ is the identity map on U, and similarly $\phi \circ \psi$ is the identity map on V. Hence ϕ is a C-algebra isomorphism of U onto V.

PROPOSITION 3.2. *Let U be a basic subalgebra of R that is stable under the left (or right) translations with the elements of G. Then* $\mathrm{Hom}(G, C) \subset U$.

Proof. Let $h \in \mathrm{Hom}(G, C)$ and write $h = \sum_{q \in Q} u_q(h) q$, with $u_q(h) \in U$. Translating on the left with an element $x \in G$, we obtain from this

$$h(x) + h = \textstyle\sum_{q \in Q} (x \cdot u_q(h)) q(x) q.$$

Comparing coefficients, we get

$$u_q(h) = (x \cdot u_q(h)) q(x), \text{ for every } q \neq 1.$$

Now evaluate at the identity element 1 of G. This yields

$$u_q(h)(1) = u_q(h)(x) q(x).$$

Thus, for every $q \neq 1$, $u_q(h) q$ is a constant. We conclude that $u_q(h) = 0$, for every $q \neq 1$, whence $h = u_1(h) \in U$, q. e. d.

In studying the algebra $R = R(G)$ of the complex valued representative functions on the (real or complex) analytic group G, we may assume (in virtue of [2, Th. 7.1] and [4, pp. 89-90]) without loss of generality that G has a faithful finite dimensional analytic representation. This assumption will be in force from now on. Let $G = H \cdot K$ be a semidirect decomposition as discussed in Section 2. Let $\mathfrak{G}$, $\mathfrak{H}$, $\mathfrak{K}$ be the Lie algebras of G, H, K, respectively. Let N be the radical of the commutator subgroup G' of G. Then $N \subset K$, and the Lie algebra $\mathfrak{N}$ of N coincides with $[\mathfrak{G}, \mathfrak{K}]$. Let $x_1, \cdots, x_m$ be a basis for $\mathfrak{N}$. Let $x_{m+1}, \cdots, x_n$ be elements of the nilpotent algebra $\mathfrak{P}$ of Lemma 2.1 such that $x_1, \cdots, x_n$ is a basis for $\mathfrak{K}$. Now every element of G can be written uniquely in the form

$$h \exp(c_n x_n) \cdots \exp(c_{m+1} x_{m+1}) \exp\left(\sum_{i=1}^{m} c_i x_i\right),$$

where $h \in H$ and the c_i are real or complex numbers (note that N is simply connected and nilpotent). We define functions $u_1, \cdots, u_n$ on G such that, for each j, the value of u_j at the element of G written above is c_j. Let S be the algebra of functions that are generated by the constants and $u_1, \cdots, u_n$. Let R^K denote the subalgebra of R that consists of the elements left fixed by the translations with the elements of K. The analysis of R made in [3, Section 4], which would be the same in the complex case as it was in the real case, has shown that $R^K S$ is a basic subalgebra of R (the notation of [3] is such that our present R^K is there denoted $R^H(G)$; the notation we adopt here is based on the principle that if W is any left module for a group A then W^A stands for the submodule of the A-fixed elements of W).

We claim that S is stable under the left translations with the elements of G. For $j > m$, we have $u_j \in \mathrm{Hom}(G, C)$, so that $g \cdot u_j = u_j(g) + u_j \in S$, for every $g \in G$. Now suppose that $j \leqq m$. Let $v \in H$. Then v commutes with every $\exp(c_k x_k)$ with $k > m$. Hence, if $t \in \mathfrak{N}$ and v^* denotes the automorphism of $\mathfrak{N}$ that corresponds to v^{-1} under the adjoint representation,

$$\begin{aligned} &h \exp(c_n x_n) \cdots \exp(c_{m+1} x_{m+1}) \exp(t) v \\ &\qquad = hv \exp(c_n x_n) \cdots \exp(c_{m+1} x_{m+1}) v^{-1} \exp(t) v \\ &\qquad = hv \exp(c_n x_n) \cdots \exp(c_{m+1} x_{m+1}) \exp(v^*(t)). \end{aligned}$$

We see at once from this that $v \cdot u_j$ is a linear combination of $u_1, \cdots, u_m$. Now let $s \in \mathfrak{N}$, and let us consider the translate $\exp(s) \cdot u_j$. The nilpotency of $\mathfrak{N}$ implies that, if $t \in \mathfrak{N}$, we have

$$\exp(t) \exp(s) = \exp(f(s, t)),$$

where f is a polynomial map of $(\mathfrak{N}, \mathfrak{N})$ into $\mathfrak{N}$. Hence it is clear that $\exp(s) \cdot u_j$ is a polynomial in $u_1, \cdots, u_m$.

There remains to consider the translates $\exp(d_k x_k) \cdot u_j$, where $k > m$ and d_k is an arbitrary real or complex number. Since $\mathfrak{P}$ is nilpotent, we have

$$\begin{aligned} &\exp(c_n x_n) \cdots \exp(c_{m+1} x_{m+1}) \exp(d_k x_k) \\ &\qquad = \exp(c_n x_n) \cdots \exp((c_k + d_k) x_k) \cdots \exp(c_{m+1} x_{m+1}) \exp(s), \end{aligned}$$

where s is a linear combination of basis elements of $[\mathfrak{P}, \mathfrak{P}]$ whose coefficients are polynomials in $c_{m+1}, \cdots, c_n$ and d_k. Writing t for $\sum_{i=1}^{m} c_i x_i$, we have

$$\begin{aligned} &h \exp(c_n x_n) \cdots \exp(c_{m+1} x_{m+1}) \exp(t) \exp(d_k x_k) \\ &= h \exp(c_n x_n) \cdots \exp((c_k + d_k) x_k) \cdots \exp(c_{m+1} x_{m+1}) \exp(s) \exp(\exp(d_k x_k)^*(t)). \end{aligned}$$

Since $s \in \mathfrak{N}$, the product of the last two factors is the exponential of $f(s, \exp(d_k x_k)^*(t))$, which is a linear combination of $x_1, \cdots, x_m$ whose coefficients are polynomials in $c_1, \cdots, c_n$ (the dependence on d_k being ignored). Hence $\exp(d_k x_k) \cdot u_j$ is a polynomial in $u_1, \cdots, u_n$.

Thus we have shown that S is stable under the left translations. Evidently, R^K is stable under the left and the right translations. Moreover, R^K is canonically isomorphic with the algebra of all representative functions on the reductive analytic group G/K. By [2, Th. 9.2] (for the real case) and [4, Th. 5.2] (for the complex case), R^K is therefore finitely generated as a C-algebra. Hence $R^K S$ is finitely generated as a C-algebra. Put $B = R^K S$.

It is easy to see (cf. [3, Section 4]) that the canonical map $R^K \otimes_C S \rightarrow R^K S$ is an isomorphism. We recall that a representative function f on G is called semisimple if the representation of G by left translations on the space spanned by the translates of f is semisimple. The semisimple elements of B constitute a subalgebra B_s of B that is stable under the left translations. We claim that $B_s = R^K$. Evidently, $R^K \subset B_s$. Conversely, let $f \in B_s$. We can write $f = \sum_{i=1}^{r} p_i s_i$, where $p_1, \cdots, p_r$ are C-linearly independent elements of R^K and the $s_i \in S$. Then we have, for every $x \in K$, $x \cdot f = \sum_{i=1}^{r} p_i (x \cdot s_i)$. Since, for given $p_1, \cdots, p_r$, this representation of $x \cdot f$ is unique, it follows that, for each i, the K-module spanned by the left K-translates of s_i is a K-homomorphic image of the K-module spanned by the left K-translates of f. Since K is normal in G, the K-module generated by f is semisimple. Hence the K-module generated by s_i is semisimple, for each i. On the other hand, N is unipotent on every finite dimensional N-submodule of R. Hence s_i must be left fixed by the left N-translations, and it follows that the restriction of s_i to K may be regarded as a representative function on the vector group K/N and, as such, is a semisimple representative function on K/N. Hence the restriction of s_i to K is a C-linear combination of elements of $\exp(\mathrm{Hom}(K/N, C))$, i.e., it coincides with the restriction to K of a C-linear combination of elements of $Q = \exp(\mathrm{Hom}(G, C))$. However, it is clear from [3, Section 4] that the restriction homomorphism $R(G) \rightarrow R(K)$ is a monomorphism on $S[Q]$. Thus we conclude that $s_i \in C[Q]$. Since the elements of Q are free over S, this implies that s_i is a constant, whence $f \in R^K$.

It is convenient to introduce the following definition: *a normal basic subalgebra of R is a basic subalgebra B such that B is stable under the left translations and B_s is stable under both the left and the right translations.*

The algebra B constructed above has been shown to be a normal basic subalgebra. Since B is finitely generated as a C-algebra, it is clear from Propostition 3.1 that *every basic subalgebra of R is finitely generated as a C-algebra.* Next, we observe that the kernel of the representation of G by left translations on B_s is the nucleus K of G. Indeed, since $B_s = R^K$, this kernel contains K. Since $G = H \cdot K$, and since the representation of H by left translations on R^K must be faithful (because H has a faithful finite dimensional representation and R^K is canonically isomorphic with the algebra of all representative functions on H), it follows that the kernel must coincide with K.

Now let D be any basic subalgebra of R that is stable under the left translations. We claim that $R_s = D_s[Q]$. Evidently, $D_s[Q] \subset R_s$. Conversely, let $f \in R_s$ and write $f = \sum_{q\in Q} d_q(f) q$, with $d_q(f) \in D$. Then we have, for every $x \in G$, $x \cdot f = \sum_{q \in Q} (x \cdot d_q(f)) q(x) q$, and $x \cdot d_q(f) \in D$. Denote by $G \cdot f$ the space spanned by the left translates of f, etc. Then $(G \cdot d_q(f))q$ is a G-homomorphic image of $G \cdot f$, for each q, and hence is semisimple. Evidently, the G-submodules of $(G \cdot d_q(f))q$ are the G-modules Vq, where V ranges over the G-submodules of $G \cdot d_q(f)$. Hence we conclude that each $d_q(f)$ is semisimple, i. e., that $d_q(f) \in D_s$. Hence $f \in D_s[Q]$, and our claim is proved.

Let ϕ denote the coefficient sum isomorphism of B onto D, as in Proposition 3.1. It follows at once from what we have just seen that $\phi(B_s) \subset D_s$. Similarly, $\phi^{-1}(D_s) \subset B_s$. Hence ϕ maps $R^K = B_s$ isomorphically onto D_s. For $x \in G$, define the map $\phi_x \colon R^K \to C$ by $\phi_x(f) = \phi(f)(x)$. Then ϕ_x is an algebra homomorphism leaving the constants fixed. Furthermore, in the real case, ϕ_x evidently commutes with the complex conjugation. By [2, Prop. 2.5], ϕ_x defines a unique proper automorphism ζ of R^K such that $\zeta(f)(1) = \phi_x(f)$. In the real case, ζ commutes with the complex conjugation. Moreover, it is clear that the map $x \to \zeta$ is continuous, so that, in the real case, ζ belongs to the connected component of the identity in the group of the real proper automorphisms of R^K. Now R^K may be regarded as the algebra of all representative functions on the reductive analytic group H. Hence it follows from [2, Th. 1.1.1] (for the real case) and [4, Th. 5.2] (for the complex case) that ζ is the left translation by an element $x_1 \in H$. Thus we have $\phi(f)(x) = f(x_1)$, for every $f \in R^K$.

Now let $d \in D_s$ and write $d = \sum_{q \in Q} f_q(d) q$, with $f_q \in B_s = R^K$. Then $d(x_1) = (\sum_{q \in Q} f_q(d))(x_1)$, because $q(x_1) = 1$, for each q, since $x_1 \in H$. Thus $d(x_1) = \phi(\sum_{q \in Q} f_q(d))(x) = d(x)$, by the proof of Proposition 3.1.

Now suppose that D is a *normal* basic subalgebra. Then, for every $d \in D_s$ and every $y \in G$, $d \cdot y \in D_s$, and hence $(d \cdot y)(x_1) = (d \cdot y)(x)$. Hence we have $x_1 \cdot d = x \cdot d$, for every $d \in D_s$. Now let L denote the kernel of the representation of G by left translations on D_s. Then our last result shows that $G = HL$. Moreover, the isomorphism $\phi\colon R^K \rightarrow D_s$ is evidently an H-module isomorphism. Since the representation of H by left translations on R^K is faithful, it follows that the representation of H by left translations on D_s is also faithful. Hence $H \cap L = (1)$, and G is the semidirect product $H \cdot L$. Clearly, $N \subset L$, and L/N is isomorphic with $G/(HN)$ and hence with K/N. Hence L is solvable. Moreover, since $H \cdot L = H \cdot K$, it follows that L is homeomorphic with K, and thus is simply connected. Hence L is a nucleus of G. Now construct a normal basic subalgebra E of R as above, but using the nucleus L. Then $E_s = R^L$, and $D_s[Q] = R_s = E_s[Q]$. Since $D_s \subset E_s$ and since the elements of Q are free over E_s, this implies that $D_s = E_s = R^L$.

We may now summarize our results as follows.

THEOREM 3.1. *Let G be an analytic group having a faithful finite dimensional analytic representation. Let R be the algebra of the representative functions on G, and let K be a nucleus of G. Then there exists a normal basic subalgebra B of R such that $B_s = R^K$ and K is the kernel of the representation of G by left translations on B_s. If D is any normal basic subalgebra of R then the kernel of the representation of G by left translations on D_s is a nucleus L of G, and $D_s = R^L$.*

We observe that *if G is solvable then every basic subalgebra of R that is stable under the left translations is a normal basic subalgebra.* Indeed, if G is solvable we have $G' = N$, so that G/N is abelian. Now if B is a left stable basic subalgebra of R then the elements of B_s are left fixed by the left translations with the elements of N. It follows that, for every $f \in B_s$ and every $x \in G$, $f \cdot x = x \cdot f$, which proves our assertion.

In general, this last result does not hold, as is shown by the following example. Let H denote the group of all 2 by 2 complex matrices with determinant 1, and let $G = H \times C$. Let α, β, γ, δ be the functions on G that associate with each element of G the entries of the matrix component of that element, so that $\alpha\delta - \beta\gamma = 1$. Let ρ be the projection of G onto C with kernel H, and put $q = \exp(\rho)$. Then it is easily seen that a left stable basic subalgebra of R is given by

$$B = C[\alpha q, \beta q, \gamma q^{-1}, \delta q^{-1}, \rho]$$

We have

$$B_s = C[\alpha q, \beta q, \gamma q^{-1}, \delta q^{-1}],$$

and one verifies directly that B_s is *not* stable under the *right* translations.

Moreover, the kernel of the representation of G by left translations on B_s is discrete, in this case, and thus is certainly not a nucleus of G.

4. Relations among normal basic subalgebras.

LEMMA 4.1. *Let B be any normal basic subalgebra of R, and let K be the kernel of the representation of G by left translations on B_s. Then* $B^N = R^K[\mathrm{Hom}(G, C)]$.

Proof. From a semidirect product decomposition $G = H \cdot K$, we see that G/N is the direct product of the reductive group $(HN)/N$ by the vector group K/N. Hence $R(G/N)$ may be identified with the tensor product of $R(G/N)^{K/N}$ and $R(G/N)^{(HN)/N}$. Now $R(G/N)^{(HN)/N}$ is canonically isomorphic with $R(K/N) = C[\mathrm{Hom}(K/N, C), \exp(\mathrm{Hom}(K/N, C)]$. Hence we have

$$R(G/N)^{(HN)/N} = C[\mathrm{Hom}(G/N, C), \exp(\mathrm{Hom}(G/N, C)].$$

Now if we apply the canonical isomorphism of $R(G/N)$ onto $R(G)^N$ we find

$$R^N = R^K \otimes_C C[\mathrm{Hom}(G, C), Q] = R^K[\mathrm{Hom}(G, C), Q].$$

Thus we have

$$R^K[\mathrm{Hom}(G, C)] \subset B^N \subset R^K[\mathrm{Hom}(G, C)][Q].$$

Since the elements of Q are free over B^N, this implies that

$$B^N = R^K[\mathrm{Hom}(G, C)].$$

Now let B be the normal basic subalgebra of R constructed from the nucleus K as in Section 3. $B = R^K[u_1, \cdots, u_n]$, and $(u_{m+1}, \cdots, u_n)$ is a C-basis for $\mathrm{Hom}(G, C)$. Hence $B = R^K[\mathrm{Hom}(G, C)][u_1, \cdots, u_m]$. Let Z denote the center of N. The elements $u_1, \cdots, u_m$ were defined with reference to a basis $x_1, \cdots, x_m$ of the Lie algebra of N. Choose this basis so that $x_1, \cdots, x_p$ is a basis for the Lie algebra of Z. Then it is clear from the definition of the functions u_i that $u_i \in B^Z$, for every $i > p$. Hence

$$B = B^Z[u_1, \cdots, u_p].$$

If we consider the natural action of the Lie algebra of Z on B, we see immediately that, for $i = 1, \cdots, p$, x_i annihilates B^Z, while $x_i(u_j) = \delta_{ij}$. Hence we see from the familiar partial differentiation argument that the monomials in the functions $u_1, \cdots, u_p$ are free over B^Z. Moreover, if we examine the argument of Section 3 with which we showed that S is stable under the left translations, we see that, actually, the free B^Z-module

$$B^Z + B^Z u_1 + \cdots + B^Z u_p$$

is stable under the left translations.

Now we are in a position to prove the following theorem.

THEOREM 4.1. *Let G be an analytic group, R the algebra of the representative functions on G. Let A and B be two normal basic subalgebras of R such that $A_s = B_s$. Then there is an element $x \in N$ such that $B \cdot x = A$.*

Proof. We make an induction on the dimension of N. Let Z be the center of N. If $Z = N$ we have $A^Z = B^Z$, by Lemma 4.1. If $Z \neq N$ we consider G/Z, identifying $R(G/Z)$ with R^Z. Then B^Z and A^Z become identified with normal basic subalgebras of $R(G/Z)$, and $(B^Z)_s = B_s = A_s = (A^Z)_s$. The radical of $(G/Z)'$ is evidently N/Z. Hence, assuming that the theorem is proved in lower dimensions (to start the induction, note that if N is trivial then $A = B$, by Lemma 4.1), there is an element $x \in N$ such that $(B^Z) \cdot x = A^Z$. Replacing A by $A \cdot x^{-1}$, we may therefore assume that $B^Z = A^Z$. Moreover, it evidently suffices to prove the theorem in the case where B is as described above, which we shall now assume.

Every element $f \in R$ may be written uniquely in the form

$$f = \textstyle\sum_{q \in Q} a_q(f) q,$$

with $a_q(f) \in A$. Then a_1 is evidently a G-module homomorphism (but not necessarily an algebra homomorphism) of R into A, and a_1 is the identity map on $B^Z = A^Z$. Let α denote the restriction of a_1 to $B^Z + B^Z u_1 + \cdots + B^Z u_p$. Since the monomials in $u_1, \cdots, u_p$ are free over B^Z, we can extend α to an *algebra* homomorphism $\beta \colon B \to A$ which, like α, commutes with the left translations. We extend β to an algebra endomorphism γ of R such that $\gamma(q) = q$, for every $q \in Q$. Clearly, γ still commutes with the left translations. Furthermore, since $\mathrm{Hom}(G, C) \subset B^Z$, γ leaves the elements of $\mathrm{Hom}(G, C)$ fixed. Hence $\gamma(\exp(f)) = \exp(\gamma(f))$, for every $f \in \mathrm{Hom}(G, C)$. Finally, we note that, in the real case, a_1 commutes with the complex conjugation, whence also γ commutes with the complex conjugation.

In the complex case, it follows at once from [4, Th. 5.1] (with left and right translations interchanged) that γ is the right translation by an element $x \in G$. Since γ leaves the elements of B^Z fixed, we have, in particular, $f \cdot x = f$, for every $f \in R^K[\mathrm{Hom}(G, C)] = B^N$. From this we conclude first that $x \in K$ (because R^K separates the elements of G/K) and then that $x \in N$ (because $\mathrm{Hom}(G, C)$ separates the elements of K/N).

In the real case, we appeal to [3, Th. 5.1] to conclude that there is an element x in the universal complexification G^+ of G such that $\gamma(f) = f \cdot x$, for every $f \in B$. Now G^+ contains the universal complexification N^+ of N, and it follows as just above, from the fact that γ leaves the elements of $R^K[\mathrm{Hom}(G, C)]$ fixed, that $x \in N^+$. Finally, since γ commutes with the complex conjugation, it follows that $x \in N$.

Thus, in either case, there is an element $x \in N$ such that $B \cdot x \subset A$. Since both $B \cdot x$ and A are basic subalgebras of R, this implies that $B \cdot x = A$, so that our theorem is proved.

Theorems 3.1 and 4.1 give a one to one correspondence between the set of nuclei of G and the set of right G-orbits of normal basic subalgebras of R. In particular, the two-sidedly G-stable subalgebras of R that are generated by the normal basic subalgebras associated with a given nucleus K of G all coincide with one and the same two-sidedly G-stable finitely generated subalgebra of R, which is thus invariantly associated with the nucleus K. In the general case, the representation-theoretical significance of this is not clarified. Moreover, this correspondence is not reversible; the same two-sidedly stable subalgebra may be associated with several, even non-isomorphic, nuclei. This is shown by the following example.

Let G be the group of 7-tuples (a, b, c, z, r, s, t), where z, r, s, t are arbitrary complex numbers, a, b, c are non-zero complex numbers, and the multiplication is given by

$$\begin{aligned}&(a, b, c, z, r, s, t)\,(a', b', c', z', r', s', t')\\ &\qquad = (aa', bb', cc', z + z', a'r + r', b's + s', c't + t').\end{aligned}$$

For every integer n, we define a nucleus K_n of G; K_n consists of the elements $(\exp(z), \exp(-z), \exp(nz), z, r, s, t)$, where z, r, s, t range over all complex numbers. We define the functions $\alpha, \beta, \gamma, \zeta, \rho, \sigma, \tau$ on G by $\alpha(a, b, c, z, r, s, t) = a$, etc. Let $q = \exp(\zeta)$. It is easily seen that R^{K_n} is generated by the functions $\alpha q^{-1}, \beta q, \gamma q^{-n}$ and their reciprocals, and that $R^{K_n}[\zeta, \rho, \sigma, \tau]$ is a normal basic subalgebra of R; in fact, it results from the construction of Section 3. Now one verifies easily that the two-sidedly stable subalgebra generated by this normal basic subalgebra is $C[\alpha, \beta, \gamma, q, q^{-1}, \alpha^{-1}, \beta^{-1}, \gamma^{-1}, \zeta, \rho, \sigma, \tau]$. This is the same for all n. On the other hand, if $n \neq 0$ then K_n is not isomorphic with K_0, because $(K_n)'$ is of dimension 3 while $(K_0)'$ is of dimension 2.

5. The unipotent hull. For our present purpose, it will be convenient to assume, to begin with, that G is a *complex* analytic group. Let A be the group of all proper automorphisms of R, and let U denote the kernel of the natural representation of A on R_s. We shall call U the *unipotent hull* of G.

We claim that, for every finite dimensional left G-stable (and hence also A-stable) subspace S of R, the natural representation of U on S is unipotent. In order to see this, let us consider a composition series $(0) = S_0 \subset S_1 \subset \cdots \subset S_k = S$ for S as a G-module. Let t_i be a linear function on S that vanishes on S_{i-1}, and let $s_i \in S_i$. Then the function t_i/s_i, where $(t_i/s_i)(x) = t_i(x \cdot s_i)$, for every $x \in G$, is a representative function associated with the representation of G on S_i/S_{i-1}, and hence belongs to R_s. Hence $u(t_i/s_i) = t_i/s_i$, for every $u \in U$, whence $t_i(u(s_i)) = t_i(s_i)$, for every $u \in U$. Since this holds for all t_i that vanish on S_{i-1} and since S_i is U-stable, this implies that $u(s_i) - s_i \in S_{i-1}$, for every $u \in U$. Hence S is unipotent as a U-module.

We may choose a finite dimensional two-sidedly stable subspace S of R such that S and the elements of Q generate R and the representation of the subgroup GU of A on S is faithful. This is done as follows: let $f_1, \cdots, f_n$ be a maximal set of linearly indpendent elements of $\mathrm{Hom}(G, C)$, and put $f_0 = c_1 f_1 + \cdots + c_n f_n$, where $c_1, \cdots, c_n$ are rationally independent complex numbers. Put $q_i = \exp(f_i)$. Then, if K is any nucleus of G, $q_0, \cdots, q_n$ separate the elements of K/N. There is a finite subset T of R containing a set of generators of R^K and such that $T \cup Q$ generates R. We let S be the smallest two-sidedly stable subspace of R that contains $\mathrm{Hom}(G, C)$, T, and $q_0, \cdots, q_n$. We claim that S satisfies our requirements.

There remains only to show that the representation of GU on S is faithful. Suppose that $x \in G$, $u \in U$, and xu leaves the elements of S fixed. Write $G = H \cdot K$, with H reductive, and $x = hk$, with $h \in H$ and $k \in K$. We have $xu(q_i) = x \cdot q_i = q_i(x) q_i = q_i(k) q_i$. Since $q_i \in S$, we have $xu(q_i) = q_i$. Hence we conclude that $q_i(k) = 1$, for $i = 0, 1, \cdots, n$. By the choice of the q_i, this implies that $k \in N$. Since $N \subset U$, this means that we may now assume that $x \in H$. If $f \in R^K$ then $f \in R_s$, so that $xu(f) = x \cdot f$. On the other hand, f belongs to the algebra generated by S, whence $xu(f) = f$. Thus $x \cdot f = f$, for every $f \in R^K$. But this implies, since $x \in H$, that $x = 1$. Now $\mathrm{Hom}(G, C) \subset S$, so that $u(f) = f$, for every $f \in \mathrm{Hom}(G, C)$. Since $\exp(f) \in R_s$, we have $u(\exp(f)) = \exp(f)$. By [4, Th. 5.1], it follows that u is the left translation by an element of G. Since S and the elements of Q generate R, this implies that $u = 1$, q. e. d.

Now let A_S and U_S denote the restrictions to S of A and U. By [2, Props. 2.6 and 2.9], A_S is the algebraic group hull of G_S. We claim that U_S coincides with the kernel, V_S say, of the semisimple representation associated with the representation of A_S on S.

In order to see this, we consider the family of all finite dimensional two-sidedly stable subspaces T of R. By the standard decomposition theorem for algebraic linear groups [5, Th. 6.1], the algebraic group A_T is a semidirect product $M_T \cdot V_T$, where M_T is fully reducible. If $T_1 \subset T_2$, the restriction from T_2 to T_1 is a rational group *epimorphism* ρ_{T_1,T_2} of A_{T_2} onto A_{T_1}. By [5, Prop. 3.2], $\rho_{T_1,T_2}(V_{T_2})$ is unipotent and $\rho_{T_1,T_2}(M_{T_2})$ is fully reducible. Hence A_{T_1} is the semidirect product of these two groups, whence it is clear that $\rho_{T_1,T_2}(V_{T_2}) = V_{T_1}$. Now let σ_{T_1,T_2} be the restriction to V_{T_2} of ρ_{T_1,T_2}, and consider the inverse system of the rational group epimorphisms σ_{T_1,T_2}. Evidently, the inverse limit of this system is precisely U. Hence we conclude from [2, Prop. 2.8] that $U_T = V_T$, for every T, which proves our above claim.

In particular, we have a semidirect decomposition $A_S = M_S \cdot U_S$, where M_S is a fully reducible group of automorphisms of S. Now we may identify GU with its image in A_S, and then we have $GU = M \cdot U$ (semidirect), where $M = M_S \cap (GU)$. Evidently, GU is a normal subgroup of A_S, whence M is a normal subgroup of M_S. Hence M is a fully reducible group of automorphisms of S. It follows that the action of M on the algebra generated by S is semisimple. Since S and the elements of Q generate R, it follows that the action of M on R is semisimple. Thus M is *R-reductive*, in the sense that R is semisimple as an M-module.

Now suppose that G is a real analytic group. In this case, we shall define the unipotent hull U of G to be the kernel of the representation on R_s of the group A_r of the *real* proper automorphisms of R, i.e., the proper automorphisms that commute with the complex conjugation. Now we choose the space S used above so as to be stable under the complex conjugation, and we consider the inverse system of the σ_{T_1,T_2} obtained by admitting only those subspaces T that are stable under the complex conjugation. Let $(A_T)_r$ be the subgroup of A_T consisting of the elements of A_T that commute with the complex conjugation of T. Then $(A_T)_r$ is a real algebraic subgroup of the group of all real linear automorphisms of T. Since A_T is the algebraic hull of $G_T \subset (A_T)_r$, it follows that the Lie algebra of A_T is the tensor product extension over C of the Lie algebra of $(A_T)_r$. Now V_T is the analytic subgroup of A_T whose Lie algebra is the set of all nilpotent elements of the radical of the Lie algebra of A_T. Hence the Lie algebra of V_T is spanned over C by the set of all nilpotent elements of the radical of the Lie algebra of $(A_T)_r$. Hence $(V_T)_r$ is the kernel of the semisimple representation associated with the representation of $(A_T)_r$ on T. By considering the corresponding Lie algebra map, we see that σ_{T_1,T_2} maps $(V_{T_2})_r$ onto all of $(V_{T_1})_r$. Now it follows from the same inverse limit argument we used above (replacing [2, Prop. 2.8] with [2, Prop. 2.11]) that $(V_T)_r = U_T$.

We may now continue exactly as in the complex case to conclude that GU is a semidirect product $M \cdot U$, where M is an R-reductive subgroup of A_r.

From now on, G may again be either complex or real. Since the analytic group M has a faithful finite dimensional semisimple analytic representation, M is a direct product $P \times V$, where V is a vector group and P is a reductive analytic group ([2, Th. 7.2] and [4, Th. 4.1]). Now $V \cdot U$ is a simply connected, solvable, normal, closed analytic subgroup of GU, and GU is the semidirect product $P \cdot (V \cdot U)$. Hence P is a maximal reductive analytic subgroup of GU.

Now we recall that if L is a linear analytic group, M a maximal fully reducible analytic subgroup of L, and T any fully reducible analytic subgroup of L, then there is an element t of the radical of L' such that $tTt^{-1} \subset M$ (see [5, Th. 4.1]).

Let K be a nucleus of G, and write $G = H \cdot K$, with H reductive. Since $(GU)_S$ lies in the algebraic hull of G_S, we have $(GU)' = G'$. Hence we may conclude from the general theorem just quoted that there is an element $t \in N$ such that $tHt^{-1} \subset P$. Since $G = tHt^{-1} \cdot K$, it follows that $G \subset MK$.

Let $x \in M$ and $y \in K$. Then $xyx^{-1}y^{-1} \in (GU)' = G'$. On the other hand, $xyx^{-1}y^{-1}$ is contained in the radical of G. Since there is a continuous arc of such commutators joining $xyx^{-1}y^{-1}$ to 1, we conclude that $xyx^{-1}y^{-1}$ lies in the connected component of the identity of the intersection of G' with the radical of G, and thus lies in the radical N of G'. Since $N \subset K$, we have therefore $xyx^{-1} \in K$. In particular, we conclude that $M \cap K$ is a normal subgroup of M. Hence $M \cap K$ is R-reductive. Since $\mathrm{Hom}(G, C)$ separates the elements of K/N, while the representation of G on $C + \mathrm{Hom}(G, C)$ is unipotent, this implies that $M \cap K \subset N$. Thus $M \cap K \subset M \cap U$, so that $M \cap K = (1)$. Hence MK is the semidirect product $M \cdot K$.

We have obtained the following result.

THEOREM 5.1. *Let G be a real or complex analytic group, and let U be the unipotent hull of G. Then GU is an analytic group having a faithful finite dimensional analytic representation, and U is a nilpotent, simply connected, normal, closed analytic subgroup of GU. There is an R-reductive closed analytic subgroup M of GU such that GU is the semidirect product $M \cdot U$. If K is any nucleus of G then G is contained in the semidirect product $M \cdot K$.*

COROLLARY 5.1. *The dimension of the unipotent hull U is equal to the dimension of any nucleus K.*

Proof. Since $U' \subset G' \cap U = N$, it is clear that U/N is a vector group.

We show first that $\mathrm{Hom}(U/N, C)$ is isomorphic with $\mathrm{Hom}(G, C)$. In doing this, we shall identify $\mathrm{Hom}(U/N, C)$ with the subgroup $\mathrm{Hom}(U, C)^N$ of $\mathrm{Hom}(U, C)$. Let $h \in \mathrm{Hom}(U, C)^N$. Since $[M, U] \subset N$, we can extend h uniquely to a homomorphism of $M \cdot U$ into C that is trivial on M. The restriction to G of this homomorphism is an element $h' \in \mathrm{Hom}(G, C)$. Clearly, the map $h \rightarrow h'$ is a linear homomorphism of $\mathrm{Hom}(U, C)^N$ into $\mathrm{Hom}(G, C)$. Conversely, given $f \in \mathrm{Hom}(G, C)$, define the map $f^*: U \rightarrow C$ by $f^*(u) = u(f)(1)$, for every $u \in U$. Since the representation of G on $(C + \mathrm{Hom}(G, C))/C$ is trivial, the same is true for the representation of U, because the image of U lies in the algebraic group hull of the image of G. From this, it is easily seen that f^* is a homomorphism, and hence that $f^* \in \mathrm{Hom}(U, C)^N$. Moreover, it is verified directly that $(f^*)' = f$ and $(h')^* = h$. Hence $\mathrm{Hom}(U/N, C)$ is isomorphic with $\mathrm{Hom}\ (G, C)$. Hence we have

$$\begin{aligned}\dim(U/N) &= \dim(\mathrm{Hom}(U/N, C))\\ &= \dim(\mathrm{Hom}(G, C)) = \dim(\mathrm{Hom}(K/N, C)) = \dim(K/N).\end{aligned}$$

Hence $\dim(U) = \dim(K)$, q. e. d.

Put $H = M \cap G$. Then, since $G \subset M \cdot K$, we have $G = H \cdot K$. Furthermore, $M' \subset G$, so that $M' \subset H$, i. e., M/H is abelian.

Now consider the natural representation of M/H on R^H. Since M is R-reductive, this is semisimple. It follows that R^H is spanned by the elements $f \in R^H$ such that, for every $x \in M$, $x(f) = \phi(x) f$, with $\phi(x) \in C$. Clearly, $\phi \in \mathrm{Hom}(M, C^*)$, where C^* is the multiplicative group of the nonzero complex numbers. Now ϕ may be regarded as an element of $\mathrm{Hom}(GU, C^*)$ that is trivial on HU. The restriction to G is trivial on HN and therefore is an element $q \in Q$. Obviously, ϕ coincides with q on GU, and so on M, i. e., $\phi(x) = x(q)(1)$, for every $x \in M$. Hence $fq^{-1} \in R^M$, and we have shown that $R^H \subset R^M[Q]$.

We denote by $f \rightarrow f'$ the involution of R defined by $f'(x) = f(x^{-1})$, for every $x \in G$. The last result is equivalent to $(R^H)' \subset (R^M)'[Q]$, and it is clear that $(R^H)'$ is the subalgebra of R consisting of all elements that are fixed under the *right* translations with the elements of H. By [2, Prop. 2.4] (taking account of the change in notation), we have $(R^H)' R^K = R$. Hence we conclude that $R^K (R^M)'[Q] = R$.

We claim that the elements of Q are free over $(R^M)'$. Let f_i be linearly independent elements of $(R^M)'$, and suppose, contrary to our claim, that there are elements $q_1, \cdots, q_n$ in Q such that $\sum_{i=1}^{n} f_i q_i = 0$. Then we have $\sum_{i=1}^{n} f_i' q_i^{-1} = 0$. Hence, for all $u \in U$ and $m \in M$,

$$\sum_{i=1}^{n} um(f_i')um(q_i^{-1}) = 0, \text{ i.e.,}$$

$$\sum_{i=1}^{n} u(f_i')m(q_i^{-1}) = 0.$$

Since the elements of U separate the f_i' (for $G \subset UM$, and the elements of M leave the f_i' fixed), we can form linear combinations of the above relations, with varying u and fixed m, so as to get $m(q_i^{-1}) = 0$, for all $m \in M$, and each i. But this is impossible, because M separates the elements of Q. This proves our above claim.

Evidently, $(R^H)'$ contains Q and $(R^M)'$. Since $(R^H)' \subset (R^M)'[Q]$, we have therefore $(R^H)' = (R^M)'[Q]$. Now R is canonically isomorphic with the tensor product of R^K and $(R^H)'$. Hence we may now conclude that the elements of Q are free over $R^K(R^M)'$. Hence $R^K(R^M)'$ is a basic subalgebra of R. Evidently, R^K and $(R^M)'$ are stable under the left translations.

We have seen in Section 3 that $R_s = D_s[Q]$, where D is any left stable basic subalgebra of R. By Theorem 3.1, we may take D so that $D_s = R^K$. Hence $R_s = R^K[Q]$. Hence $(R^K(R^M)')_s \subset R^K[Q]$. But this implies that $(R^K(R^M)')_s = R^K$. Hence we have the following result.

THEOREM 5.2. *Let G, M, K be as in Theorem 5.1. Then $R^K(R^M)'$ is a normal basic subalgebra of R, and K is the associated nucleus of G.*

It is clear from Theorem 4.1 that every normal basic subalgebra of R has the form of Theorem 5.2; right translation by $x \in N$ changes M to $x^{-1}Mx$.

6. The group of the proper automorphisms. Let A denote the group of all proper automorphisms of R, let K be a nucleus of G, and let W denote the subgroup of A consisting of all elements of A that leave the elements of R^KR^M fixed. In the complex case, let P stand for the natural image of G in A. In the real case, let P stand for the natural image of G^+ in A. Then P is a closed normal subgroup of A. In fact, by [3, Th. 5.1], P is the group of all *perfect* automorphisms of R, i.e., the proper automorphisms α such that $\exp(\alpha(f)) = \alpha(\exp(f))$, for every $f \in \mathrm{Hom}(G, C)$. We claim that A is the semidirect product $W \cdot P$. Since $R^KR^M[Q] = R$ and $\mathrm{Hom}(G, C) \subset R^KR^M$, it is clear that $P \cap W = (1)$. Hence it suffices to show that $A = WP$. Let $\phi \in \mathrm{Hom}(Q, C^*)$. Since the elements of Q are free over R^KR^M and since R^KR^M is stable under the right translations, there is one and only one element $\alpha_\phi \in W$ such that $\alpha_\phi(q) = \phi(q)q$, for every $q \in Q$. Clearly, the map $\phi \rightarrow \alpha_\phi$ is an isomorphism of $\mathrm{Hom}(Q, C^*)$ onto W.

Now let β be an arbitrary element of A. Let β' denote the homomorphism of R into C that is given by $\beta'(r) = \beta(r)(1)$, for every $r \in R$. For every $q \in Q$, there is one and only one $f \in \mathrm{Hom}(G, C)$ such that $q = \exp(f)$. Hence there is an element $\phi \in \mathrm{Hom}(Q, C^*)$ such that

$$\phi(\exp(f)) = \exp(\beta'(f))[\beta'(\exp(f))]^{-1},$$

for every $f \in \mathrm{Hom}(G, C)$. One verifies directly that the automorphism $\alpha_\phi \circ \beta$ of R is a perfect automorphism, so that $\alpha_\phi \circ \beta \in P$. Hence $\beta \in WP$, so that $A = WP$.

We observe also that the elements of W commute with the elements of M, and hence with the elements of the maximal reductive analytic subgroup $H = M \cap G$ of G. In the real case, we note that H^+ is a maximal reductive analytic subgroup of G^+; $G^+ = H^+ \cdot K^+$, and the elements of W still commute with the elements of H^+. Hence we may state our result as follows

THEOREM 6.1. *The group A of the proper automorphisms of R is a semidirect product $W \cdot P$, where P is the natural image of G (in the complex case) or of G^+ (in the real case) in A, and W is isomorphic, via restriction to Q, with* $\mathrm{Hom}(Q, C^*)$. *Moreover, the elements of W commute with the elements of some maximal reductive analytic subgroup of P.*

Let S be a finite dimensional two-sidedly stable subspace of R such that the natural representation σ of P on S is faithful. Let $E(S)$ denote the algebra of all linear endomorphisms of S. We know that the natural image A_S of A in $E(S)$ is the algebraic group hull of $P_S = \sigma(P)$. Let $\mathfrak{P}$ denote the Lie algebra of P. We may identify $\mathfrak{P}$ with its image $\sigma^{\cdot}(\mathfrak{P})$ in $E(S)$, where $\sigma^{\cdot}$ is the differential of σ. Now let α denote the adjoint representation of P in $E(\mathfrak{P})$. If we identify $\mathfrak{P}$ with $\sigma^{\cdot}(\mathfrak{P})$ then, for every $p \in P$, $\alpha(p)$ becomes identified with the conjugation $\zeta \to \sigma(p)\zeta\sigma(p)^{-1}$ in the algebra $E(\sigma^{\cdot}(\mathfrak{P}))$ of all linear endomorphisms of $\sigma^{\cdot}(\mathfrak{P})$. Since A_S is the algebraic group hull of $\sigma(P)$, $\sigma^{\cdot}(\mathfrak{P})$ is stable also under the conjugations with the elements of A_S, and the corresponding image of A_S in $E(\sigma^{\cdot}(\mathfrak{P}))$ is the algebraic group hull of $\alpha(P)$. Transferred back to $E(\mathfrak{P})$, this means the following: the conjugation of P effected by an element of A is an analytic automorphism of P and determines a Lie algebra automorphism of $\mathfrak{P}$. We shall call the resulting representation of A in $E(\mathfrak{P})$ the adjoint representation of A on $\mathfrak{P}$. Our result is that this sends A onto the algebraic group hull of the adjoint group of P, i.e., *the adjoint representation of A on the Lie algebra of P sends A onto the algebraic group hull of the adjoint group of P.*

It is an immediate corollary that if $Z(P)$ is the centralizer of P in A then $A = Z(P)P$ *if and only if the adjoint group of P is algebraic.*

However, the following example shows that, even when $A = Z(P)P$, P need not be a direct factor in A. Let G be the group of all pairs (a, b) of complex numbers, with the multiplication

$$(a, b)(a', b') = (a + a', b + \exp(a)b').$$

A right stable basic subalgebra B of R is generated by the constants and the two functions u_1, u_2, where

$$u_1(a, b) = b, \text{ and } u_2(a, b) = a.$$

The translates of these functions are as follows:

$$u_1 \cdot (a, b) = b + \exp(a)u_1; \qquad (a, b) \cdot u_1 = u_1 + b\exp(u_2);$$
$$u_2 \cdot (a, b) = a + u_2 = (a, b) \cdot u_2.$$

In this case, a subgroup W of A as in Theorem 6.1 can be described explicitly as follows: for every $\gamma \in \mathrm{Hom}(C, C^*)$, there is a $\gamma^* \in W$ defined by:

$$\gamma^*(b) = b, \text{ for every } b \in B, \text{ and}$$
$$\gamma^*(\exp(cu_2)) = \gamma(c)\exp(cu_2) \text{ for every } c \in C.$$

The functions $\exp(cu_2)$ make up the group $Q = \exp(\mathrm{Hom}(G, C))$. Let $t(a, b)$ denote the left translation by (a, b) on R. Then one verifies easily that

$$\gamma^* t(a, b) \gamma^{*-1} = t(a, \gamma(1)b).$$

On the other hand,

$$(a', b')(a, b)(a', b')^{-1} = (a, b' + \exp(a')b - \exp(a)b').$$

Hence the conjugation with γ^* on P is the conjugation with $t(a', b')$ if and only if, for all a and b,

$$\gamma(1)b = (1 - \exp(a))b' + \exp(a')b,$$

i.e., if and only if $b' = 0$ and $\exp(a') = \gamma(1)$.

In particular, we conclude that $A = Z(P)P$. We shall see, however, that P is not a direct factor in A. Indeed, suppose that P is a direct factor in A. Then there is a homomorphism $\phi \colon W \to P$ such that $\gamma^*\phi(\gamma^*)^{-1} \in Z(P)$, for every $\gamma \in \mathrm{Hom}(C, C^*)$. Putting $\phi(\gamma^*) = t(a_\gamma, b_\gamma)$, we see from the above that we must have $b_\gamma = 0$ and $\exp(a_\gamma) = \gamma(1)$. The map $\gamma \to a_\gamma$ is therefore a homomorphism $\sigma \colon \mathrm{Hom}(C, C^*) \to C$ such that $\exp(\sigma(\gamma)) = \gamma(1)$, for every $\gamma \in \mathrm{Hom}(C, C^*)$.

For each $a \in C$, define the element $\exp_a$ of $\mathrm{Hom}(C, C^*)$ by $\exp_a(c)$

$= \exp(ac)$, for every $c \in C$. The map $a \to \sigma(\exp_a)$ is an endomorphism ψ of C. Since $\exp(\psi(a)) = \exp(a)$, we conclude that $\psi(a) - a$ is an integral multiple of $2\pi i$, for every $a \in C$. Evidently, this implies that $\psi(a) = a$, for every $a \in C$, i.e., $\sigma(\exp_a) = a$. It follows from this that $\mathrm{Hom}(C, C^*)$ is the direct product of the subgroup consisting of the $\exp_a$ and the kernel, H say, of σ.

If n is any positive integer then, for every $\gamma \in \mathrm{Hom}(C, C^*)$, there is one and only one $\gamma_n \in \mathrm{Hom}(C, C^*)$ such that $(\gamma_n)^n = \gamma$; in fact, $\gamma_n(c) = \gamma(c/n)$, for every $c \in C$. It follows that if $h \in H$ then also $h_n \in H$. Since $h(1) = 1$, for every $h \in H$, we conclude that $h(q) = 1$, for every rational number q. Hence every $\gamma \in \mathrm{Hom}(C, C^*)$ coincides on the group Q of the rational numbers with an $\exp_a$. But this is a contradiction. For instance, write $C = Q + D$, where D is a Q-subspace of C such that $Q \cap D = (0)$. Define the element γ of $\mathrm{Hom}(C, C^*)$ as follows: $\gamma(d) = 1$, for every $d \in D$; $\gamma(q) = 1$, for every rational number q that can be written with an odd denominator; $\gamma(q) = \exp(2\pi i q)$, whenever q can be written with a power of 2 as denominator. Since this γ does not coincide with an $\exp_a$ on Q, we have reached a contradiction. Thus P is not a direct factor of A.

7. Representations as a closed subgroup of a full linear group.

The existence of a right stable basic subalgebra of R leads to a simple proof of the following result which extends (to the complex case) and sharpens a result due to Goto [1, Th. 9].

THEOREM 7.1. *Let G be a real or complex analytic group, and let ρ be an analytic representation of G with finite dimensional representation space V. Then there is a finite dimensional analytic representation σ with representation space W such that $V \subset W$ (as a G-module) and $\sigma(G)$ is closed in the group of all linear automorphisms of W.*

Proof. Let B denote a right stable basic subalgebra of R. We can find a finite dimensional subspace S of R satisfying the following conditions:

(1) S is two-sidedly stable and, in the real case, S is stable under the complex conjugation;

(2) the elements of S, together with the constants, generate a subalgebra of R containing B;

(3) S contains $\mathrm{Hom}(G, C)$ and the representative functions associated with the given representation ρ;

(4) if $s \in S$, and $s = \sum_{q \in Q} b_q(s) q$, with $b_q(s) \in B$ then every $q \in Q$ for which $b_q(s) \neq 0$ belongs to S.

In fact, we can evidently find a finite dimensional subspace S_1 of R satisfying conditions (1), (2) and (3). Let S_2 be the space of the C-linear combinations of the elements of Q that occur with non-zero coefficients in the expressions for the elements of S_1 as B-linear combinations of elements of Q. Since S_1 is finite dimensional, so is S_2, and if $S = S_1 + S_2$ then S satisfies all the above conditions.

Now consider the representation, ϕ say, of G by left translations on S. We claim that $\phi(G)$ is closed in the group of all linear automorphisms of S. Let A denote the group of all proper automorphisms of R, and let A_S be its natural image in the group of all linear automorphisms of S. Since A_S is the algebraic group hull of $\phi(G)$, it is closed in the full linear group. Hence it suffices to show that $\phi(G)$ is closed in A_S. We define a closed subgroup T of A_S as follows: in the complex case, T consists of all $\beta \in A_S$ such that $\beta(\exp(f)) = \exp(\beta(f))$, whenever $f \in \mathrm{Hom}(G, C)$ and $\exp(f) \in S$; in the real case, T consists of all the elements $\beta \in A_S$ satisfying this condition and commuting with the complex conjugation. Now let α be an element of A whose restriction to S belongs to T. We can define an algebra endomorphism α^* of R such that α^* coincides with α on B, while $\alpha^*(\exp(f)) = \exp(\alpha(f))$, for every $f \in \mathrm{Hom}(G, C)$. Since B is stable under the right translations, it is clear that α^* commutes with the right translations. Hence [2, Prop. 2.5] α^* is a proper automorphism of R, and hence a perfect automorphism of R. Moreover, in the real case, α^* evidently commutes with the complex conjugation, so that α^* is a real perfect automorphism. Clearly, because of (4), α^* coincides with α on S. Hence we conclude that, in the complex case, $T = \phi(G)$. In the real case, we conclude that T is the restriction image of the group P_r of all real perfect automorphisms. It is clear from [3, Th. 5.1] that $\phi(G)$ is the connected component of the identity in $(P_r)_S$. Thus, in either case, $\phi(G)$ is closed in T, and therefore also in the full linear group.

Finally, if n is the dimension of V over C, V may be identified with a G-submodule of the direct sum of n copies of S, by condition (3) and [2, Prop. 2.3]. If we take W to be the direct sum of n copies of S and let σ be the representation of G on W obtained from ϕ in the natural fashion then σ evidently satisfies the requirements of Theorem 7.1.

8. Nilpotent nuclei and algebraic structures.

THEOREM 8.1. *Let G be a real or complex analytic group, B a normal basic subalgebra of R, K the nucleus of G that is associated with B. Then B is two-sidedly stable if and only if K is nilpotent. Moreover, in that case,* *B coincides with the algebra of all representative functions associated with representations that are unipotent on K.*

Proof. Suppose first that B is two-sidedly stable. By definition, K is the kernel of the representation of G on B_s. Let S be any left stable finite dimensional subspace of B. Since B is two-sidedly stable, all the representative functions associated with the representation of G on S belong to B. Hence we may apply the argument of the beginning of Section 5 (used there for showing that the representation of U on S is unipotent) to conclude that the representation of K on S is unipotent. Since B is a basic subalgebra of R, we may choose S so that the representation of K (even of G) on S is faithful. Hence we conclude that K is nilpotent.

Now suppose that K is nilpotent. Let B_1 be the normal basic subalgebra of R constructed from K as in Section 3. It has been shown in [3, pp. 304-306] that the nilpotency of K implies that B_1 coincides with the algebra of all representative functions associated with representations that are unipotent on K. Hence B_1 is two-sidedly stable, and it follows from Theorem 4.1 that $B_1 = B$. This completes the proof of Theorem 8.1.

Remark. Let H be a maximal reductive analytic subgroup of G, and let U be the unipotent hull of G. Since H is determined up to a conjugation with an element of N, the subgroups HU and HN of A are independent of the particular choice of H. Now *suppose that G has a nilpotent nucleus K, and let B be the corresponding two sidedly stable basic subalgebra of R.* We claim that *B uniquely determines an analytic isomorphism of HU onto G that sends U onto K and leaves the elements of HN fixed.* In order to see this, we consider the natural representations of HU and G by proper automorphisms of B. Since HU leaves the elements of Q fixed, it is clear that the representation of HU on B is faithful. On the other hand, we know that the representation of G on B is faithful, and that K is the kernel of the representation of G on B_s. Hence the image of K in the group of the proper automorphisms of B must contain the image of U. By Corollary 5.1, we have $\dim(K) = \dim(U)$. Hence we conclude that the images of U and of K in the group of the proper automorphisms of B coincide. Evidently, this suffices to establish our claim; the isomorphism between HU and G goes via the group of the proper automorphisms of B.

Observe that this result immediately implies Theorem 8.4 below; however, we shall give a more direct proof of Theorem 8.4 later on, because this will lead to an explicit description of the set of all nilpotent nuclei.

Now let G be a complex analytic group, and suppose that G has a faithful complex analytic representation ρ such that $\rho(G)$ is an algebraic linear group. Let B_ρ denote the subalgebra of R consisting of all $f \in R$ such that $f \circ \rho^{-1}$ is a rational function on $\rho(G)$. If σ is another such representation of G then $B_\rho = B_\sigma$ if and only if the representation $\sigma \circ \rho^{-1} \colon \rho(G) \rightarrow \sigma(G)$ is a rational representation of $\rho(G)$. In order to see this, we need only observe that the representation $\sigma \circ \rho^{-1}$ is rational if and only if its inverse $\rho \circ \sigma^{-1}$ is rational [2, Lemma 10.2]. We shall call such a subalgebra B_ρ of R an *algebraic structure* of G. If S is any finite dimensional left stable subspace of B_ρ whose elements, together with the constants, generate B_ρ then the representation of G on S is a faithful representation of G yielding a faithful rational representation of $\rho(G)$, so that the image is an algebraic group, rationally isomorphic with $\rho(G)$. By [2, Lemma 10.1], such a subspace exists in every B_ρ. Thus the subalgebras B_ρ correspond in a 1-1 fashion to the rational isomorphism classes of the faithful representations of G as an algebraic linear group.

We shall see that the algebraic structures of G are precisely the two-sidedly stable basic subalgebras of R. This will follow easily from the next theorem.

THEOREM 8.2. *Let G be a complex analytic group, and let ρ be a faithful complex analytic representation of G such that $\rho(G)$ is an algebraic linear group. Let K be the kernel of the semisimple representation associated with ρ. Then K is a nilpotent nucleus of G, and a complex analytic representation σ of G yields a rational representation $\sigma \circ \rho^{-1}$ of $\rho(G)$ if and only if σ is unipotent on K.*

Proof. Let ρ' denote the semisimple representation associated with ρ. Clearly, $\rho' \circ \rho^{-1}$ is a rational representation of the algebraic group $\rho(G)$. Hence its kernel, $\rho(K)$, is an algebraic subgroup of $\rho(G)$. Since $\rho(K)$ is unipotent, this implies that $\rho(K)$ is connected, simply connected, and nilpotent. Hence K is connected, simply connected, and nilpotent. On the other hand, $\rho'(G)$ is a fully reducible linear algebraic group, and it follows from [4, Th. 4.1] that $\rho'(G)$ is therefore a reductive complex analytic group. Since G/K is isomorphic with $\rho'(G)$, it is now clear that K is a nilpotent nucleus of G.

Now write G as a semidirect product $H \cdot K$, with H reductive. Consider the corresponding decomposition $\rho(G) = \rho(H) \cdot \rho(K)$. Let V be the representation space of ρ, and let $(0) = V_0 \subset \cdots \subset V_n = V$ be a composition series of V. Since $\rho(H)$ is fully reducible, there is a $\rho(H)$-module isomorphism $\phi \colon \sum_{i=1}^{n} V_i/V_{i-1} \rightarrow V$. Consider the algebra isomorphism $\psi \colon e \rightarrow \phi \circ e \circ \phi^{-1}$

of $E(\sum_{i=1}^{n} V_i/V_{i-1})$ onto $E(V)$. The representation of G on $\sum_{i=1}^{n} V_i/V_{i-1}$ is the semisimple representation ρ' associated with ρ, and $\rho' \circ \rho^{-1}$ is the rational representation of $\rho(G)$ on $\sum_{i=1}^{n} V_i/V_{i-1}$. Now $\psi \circ \rho' \circ \rho^{-1}$ is precisely the projection of $\rho(G)$ onto $\rho(H)$ that corresponds to the decomposition $\rho(G) = \rho(H) \cdot \rho(K)$. Hence it is clear that this projection is a rational group epimorphism of the algebraic group $\rho(G)$ onto the algebraic group $\rho(H)$. It follows that the projection of $\rho(G)$ onto $\rho(K)$ is also a rational map (though not necessarily a group homomorphism).

Now let σ be a complex analytic representation of G. If $\sigma \circ \rho^{-1}$ is a rational representation of $\rho(G)$ then it is unipotent on $\rho(K)$, by [5, Prop. 3. 2]. Thus σ is unipotent on K, in that case. Conversely, suppose that σ is unipotent on K, and let f be a representative function associated with σ. It follows from the elementary theory of representative functions (see [2, Section 2]) that there are representative functions u_i on H and representative functions v_i on K such that the u_i are associated with the restriction of σ to H, the v_i are associated with the restriction of σ to K, and $f(hk) = \sum_{i=1}^{n} u_i(h) v_i(k)$, for all $h \in H$ and $k \in K$. The functions $u_i \circ \rho^{-1}$ are analytic representative functions on $\rho(H)$ and, since $\rho(H)$ is reductive, they are rational functions on $\rho(H)$, by [4, Th. 5. 2]. Since σ is unipotent on K, the restriction of $\sigma \circ \rho^{-1}$ to $\rho(K)$ is a rational representation of the unipotent algebraic group $\rho(K)$. Hence the functions $v_i \circ \rho^{-1}$ are rational functions on $\rho(K)$. Since the projections of $\rho(G)$ onto $\rho(H)$ and $\rho(K)$ are rational maps, we may now conclude that $f \circ \rho^{-1}$ is a rational representation of $\rho(G)$. This completes the proof of Theorem 8. 2.

It is clear from Theorems 8. 1 and 8. 2 that each algebraic structure B_ρ is a two-sidedly stable basic subalgebra of R, and that the associated nucleus K is the kernel of the semisimple representation associated with ρ. Conversely, let B be any two-sidedly stable basic subalgebra of R. It is easily seen, as in our proof of Theorem 6. 1, that every proper automorphism of R coincides on B with a left translation by an element of G. Let S be a finite dimensional two-sidedly stable subspace of B whose elements, together with the constants, generate B. Let ρ be the representation of G by left translations on S. Then $\rho(G) = A_S$ and hence, by [2, Props. 2. 6 and 2. 9], $\rho(G)$ is an algebraic subgroup of the group of all linear automorphisms of S. Now $B \subset B_\rho$, and since B_ρ is a basic subalgebra of R this implies that $B = B_\rho$. Thus we have the following result.

THEOREM 8.3. *Let G be a complex analytic group. Then the algebraic structures of G are precisely the two-sidedly stable basic subalgebras of R. This gives a 1-1 correspondence between the algebraic structures and the nilpotent nuclei of G, as follows: given an algebraic structure on G, the corresponding nilpotent nucleus is the largest normal subgroup of G on which every rational representation of G (belonging to the given algebraic structure) is unipotent; given a nilpotent nucleus of G, the rational representations for the corresponding algebraic structure are precisely those complex analytic representations of G which are unipotent on the given nucleus.*

In view of Theorem 8.3, it is of interest to examine the set of the nilpotent nuclei of G. A description of this set is made possible by the fact, discovered by B. Kostant, that any two *nilpotent* nuclei of G are conjugate by an analytic automorphism of G (note that the example at the end of Section 4 shows that this is false for non-nilpotent nuclei). We observe first that it follows from the conjugacy (by inner automorphisms) of any two maximal reductive analytic subgroups of an analytic group that, if K is a nucleus of G and H is *any* maximal reductive analytic subgroup of G, then G is the semidirect product $H \cdot K$.

THEOREM 8.4 (B. Kostant). *Let G be a real or complex analytic group, and suppose that K and L are two nilpotent nuclei of G. Let H be a maximal reductive analytic subgroup of G, so that $G = H \cdot K = H \cdot L$. Then there is an analytic automorphism α of G such that α leaves the elements of HN fixed and $\alpha(K) = L$.*

Proof. Let $\mathfrak{G}$ be the Lie algebra of G, $\mathfrak{M}$ the maximum nilpotent ideal of $\mathfrak{G}$, $\mathfrak{H}$ the Lie algebra of H, $\mathfrak{K}$ and $\mathfrak{L}$ the Lie algebras of K and L. We have $\mathfrak{G} = \mathfrak{H} + \mathfrak{L}$, the sum being semidirect, and $\mathfrak{L} \subset \mathfrak{M}$. Hence $\mathfrak{M} = \mathfrak{H} \cap \mathfrak{M} + \mathfrak{L}$.

Under the adjoint representation of G on $\mathfrak{G}$, H operates semisimple on $\mathfrak{G}$. Let M be the maximum nilpotent normal analytic subgroup of G. Then $H \cap M$ is normal in H, and hence operates semisimply on $\mathfrak{G}$. On the other hand, M operates unipotently on $\mathfrak{G}$. Hence we conclude that $H \cap M$ operates trivially on $\mathfrak{G}$. Hence $H \cap M$ lies in the center of G and $\mathfrak{H} \cap \mathfrak{M}$ lies in the center of $\mathfrak{G}$.

For $x \in \mathfrak{K}$, write $x = \zeta(x) + \gamma(x)$, with $\zeta(x) \in \mathfrak{H} \cap \mathfrak{M}$ and $\gamma(x) \in \mathfrak{L}$. Now, if $u \in \mathfrak{G}$, write $u = v + x$, with $v \in \mathfrak{H}$ and $x \in \mathfrak{K}$, and define $f(u) = v + \gamma(x)$. Since γ is a linear isomorphism of $\mathfrak{K}$ onto $\mathfrak{L}$, f is a linear automorphism of $\mathfrak{G}$. Since $\mathfrak{H} \cap \mathfrak{M}$ is in the center of $\mathfrak{G}$, we have $[x, y] = [\gamma(x), y]$, for every $x \in \mathfrak{K}$ and every $y \in \mathfrak{G}$, whence $[f(u), y] = [u, y]$, for all u and y in $\mathfrak{G}$. Hence $[f(u_1), f(u_2)] = [u_1, u_2]$, for all u_1, u_2 in $\mathfrak{G}$. But $[\mathfrak{G}, \mathfrak{G}] \subset \mathfrak{H} + \mathfrak{K} \cap \mathfrak{L}$, because both $\mathfrak{K}$ and $\mathfrak{L}$ must contain the radical of $[\mathfrak{G}, \mathfrak{G}]$. Hence f is the identity map on $[\mathfrak{G}, \mathfrak{G}]$, so that the above implies that f is a Lie algebra automorphism of $\mathfrak{G}$.

Now let H^* be the universal covering group of H. Then the appropriately defined semidirect product $H^* \cdot K$ (in which H^* operates on K via H) is the universal covering group of G. Hence our automorphism f of $\mathfrak{G}$ defines an analytic automorphism f^* of $H^* \cdot K$. Since f leaves the elements of $\mathfrak{H}$ fixed, f^* leaves the elements of H^* fixed. Hence f^* induces an automorphism α on $G = H \cdot K$ such that α leaves the elements of H fixed and coincides with f^* on K. Since f maps $\mathfrak{K}$ onto $\mathfrak{L}$ and coincides with the identity map on $\mathfrak{N}$, it follows that $\alpha(K) = L$ and that α leaves the elements of HN fixed. This completes the proof.

As an immediate consequence of Theorems 8.3 and 8.4, we obtain the following result.

THEOREM 8.5. *Let S and T be two complex linear irreducible algebraic groups, and suppose that σ is a complex analytic isomorphism of S onto T. Then there exists a complex analytic automorphism α of S such that $\sigma \circ \alpha$ is a rational isomorphism of S onto T.*

Proof. Let $B(S) \subset R(S)$ and $B(T) \subset R(T)$ be the given algebraic structures of S and T, respectively. Then $B(T) \circ \sigma$ is also an algebraic structure of the analytic group S. Let L and K be the nilpotent nuclei of S that correspond to $B(T) \circ \sigma$ and $B(S)$, respectively. There is an analytic automorphism α of S such that $\alpha(K) = L$. This implies that $B(T) \circ \sigma \circ \alpha = B(S)$, i.e., that $\sigma \circ \alpha$ is a rational isomorphism of S onto T.

It is known from the theory of Abelian varieties that Theorem 8.5 does not extend to general (non-linear) complex algebraic groups.

Now we proceed to describe the set of all nilpotent nuclei of the real or complex analytic group G. As before, let N denote the radical of G', and let M be the maximum nilpotent normal analytic subgroup of G. Let $\mathfrak{N}$ and $\mathfrak{M}$ be the Lie algebras of N and M, respectively. Let H be a maximal reductive analytic subgroup of G. We have seen in the proof of Theorem 8.4 that $H \cap M$ lies in the center of G. Since the maximal reductive analytic subgroups of G are conjugate under inner automorphisms, it follows that $H \cap M$ is actually independent of the choice of H, and thus is a uniquely determined closed central subgroup P of G. Let $\mathfrak{P}$ denote the Lie algebra of P. We denote by $\mathrm{Hom}(\mathfrak{M}/(\mathfrak{P} + \mathfrak{N}), \mathfrak{P})$ the space of all linear maps of $\mathfrak{M}$ into $\mathfrak{P}$ that send $\mathfrak{P} + \mathfrak{N}$ onto (0). Finally, let T denote the radical of G.

THEOREM 8.6. *Let G be a real or complex analytic group. Then G has a nilpotent nucleus if and only if T/M is reductive. In that case, the set* *of all nilpotent nuclei of G has the structure of an affine space, with* $\mathrm{Hom}(\mathfrak{M}/(\mathfrak{P}+\mathfrak{N}),\mathfrak{P})$ *as the underlying vector group.*

Proof. In the real case, [3, Th. 5.3] implies that there is a two-sidedly stable basic subalgebra of R if and only if T/M is reductive. In the complex case, the same result is contained in [4, Th. 5.4]. Hence the first statement of Theorem 8.6 follows from Theorem 8.1.

Now let K be a nilpotent nucleus of G, and write $G = H\cdot K$, as before. If $\mathfrak{K}$ is the Lie algebra of K then, as we have seen in the proof of Theorem 8.4, $\mathfrak{M}$ is the semidirect sum $\mathfrak{P}+\mathfrak{K}$. Now let $\phi \in \mathrm{Hom}(\mathfrak{M}/(\mathfrak{P}+\mathfrak{N}),\mathfrak{P})$. Let $\mathfrak{L}$ be the subspace of $\mathfrak{M}$ consisting of the elements $\phi(x)+x$, where x ranges over $\mathfrak{K}$. Noting that $\mathfrak{P}$ lies in the center of $\mathfrak{G}$ and that ϕ annihilates $[\mathfrak{G},\mathfrak{K}]$, we see that $\mathfrak{L}$ is an ideal of $\mathfrak{G}$. Clearly, $\mathfrak{H}+\mathfrak{L}=\mathfrak{H}+\mathfrak{K}=\mathfrak{G}$, and $\mathfrak{H}\cap\mathfrak{L} = (0)$. The proof of Theorem 8.4 shows that there is an analytic automorphism α of G such that α leaves the elements of H fixed and $\alpha(K)$ is the analytic subgroup L of G whose Lie algebra is $\mathfrak{L}$. Thus L is a nilpotent nucleus of G. We write $L=\phi\cdot K$. One checks immediately from the definition that, if ψ is any other element of $\mathrm{Hom}(\mathfrak{M}/(\mathfrak{P}+\mathfrak{N}),\mathfrak{P})$, then $\phi\cdot(\psi\cdot K) = (\phi+\psi)\cdot K$, and that $0\cdot K = K$. Moreover, $\phi\cdot K = K$ implies that $\phi = 0$, because $\mathfrak{M}=\mathfrak{P}+\mathfrak{K}$. Finally, it is clear from the proof of Theorem 8.4 (where we introduced the map ζ) that, given K and L, there is an element ϕ in $\mathrm{Hom}(\mathfrak{M}/(\mathfrak{P}+\mathfrak{N}),\mathfrak{P})$ such that $\phi\cdot L = K$. This completes the proof of Theorem 8.6.

In particular, we note that G has only one nilpotent nucleus if and only if either $\mathfrak{P}=(0)$ or $\mathfrak{P}+\mathfrak{N}=\mathfrak{M}$. The first alternative means that M is a nucleus. The second alternative means that N is a nucleus, i.e., that G/G' is reductive (see [4, Th. 5.2] and [2, Ths. 11.1 and 9.1]).

It is clear from Theorem 8.3 that, if G is a complex analytic group, Theorem 8.6 describes the algebraic structures of G, simply by reading 'algebraic structure' for 'nilpotent nucleus,' throughout.

REFERENCES.

[1] M. Goto, "Faithful representations of Lie groups II," *Nagoya Mathematical Journal*, vol. 1 (1950), pp. 91-107.

[2] G. Hochschild and G. D. Mostow, "Representations and representative functions of Lie groups," *Annals of Mathematics*, vol. 66 (1957), pp. 495-542.

[3] ———, II, *ibid.*, vol. 68 (1958), pp. 295-313.

[4] ———, III, *ibid.*, vol. 70 (1959), pp. 85-100.

[5] G. D. Mostow, "Fully reducible subgroups of algebraic groups," *American Journal of Mathematics*, vol. 78 (1956), pp. 200-221.

LINEARE GRUPPEN ÜBER LOKALEN RINGEN.*

Von Wilhelm Klingenberg.

1. Resultate.†

1.1. Wir betrachten einen (kommutativen) lokalen Ring L. Das grösste Ideal von L wird mit I bezeichnet. Dan ist $L^* = L - L$ eine Gruppe unter der Multiplikation. Falls J ein Ideal in L ist, $J \neq L$, so ist L/J wieder ein lokaler Ring. Es bezeichne

$$g_J : L \rightarrow L/J \tag{1}$$

den natürlichen Homomorphismus von L auf L/J.

Unter einem *n-dimensionalen Vektorraum über* L, $V = V_n(L)$, verstehen wir einen L-Modul isomorph zu L^n. Unter einem *m-dimensionalen Unterraum von* V verstehen wir einen Untermodul U von V, der direkter Summand ist und isomorph zu L^m.

Die *allgemeine lineare Gruppe in n Variablen über* L, $GL(n,L)$, ist definniert als die Gruppe der lineare Automorphismen von $V = V_n(L)$.

Sei J ein Ideal in L. (1) bestimmt den natürlichen Homomorphismus

$$g_J : V_n(L) \rightarrow V_n(L/J). \tag{2}$$

Hier lassen wir auch $J = L$ zu; in diesem Falle soll $V_n(L/J)$ den 0-Vektorraum bezeichnen. (2) bestimmt den natürlichen Homomorphismus

$$h_J : GL(n,L) \rightarrow GL(n,L/J) \tag{3}$$

mit der Eigenschaft $(h_J\sigma)g_J = g_J\sigma$ für alle $\sigma \in GL(n,L)$. Im Falle $J = L$ soll $GL(n,L/J)$ die Einheitsgruppe E sein. Unter der *Ordnung* $o(X)$ eines Vektors $X \in V_n(L)$ verstehen wir das kleinste Ideal J mit $g_J X = 0$. Unter der *Ordnung* $o(\sigma)$ eines Elements $\sigma \in GL(n,L)$ verstehen wir das kleinste Ideal J so, dass $h_J\sigma \in$ Zentrum $GL(n,L/J)$. Unter der *Ordnung* $o(G)$ einer Untergruppe G von $GL(n,L)$ verstehen wir das kleinste Ideal J so dass $h_J G \subset$ Zentrum $GL(n,L/J)$.

Sei E_i, $1 \leqq i \leqq n$, eine Basis von V. Wenn, für $X \in V$, $X = \sum E_i x_i$, so ist $o(X)$ gleich dem von den x_i, $1 \leqq i \leqq n$, erzeugten Ideal. Wenn, für

---

* Received September 19, 1960.

† Die wichtigsten Resultate der Arbeit wurden angekündigt in [6].

$\sigma \in GL(n,L)$, $\sigma E_j = \sum E_i a_{ij}$, so ist $o(\sigma)$ gleich dem von den a_{ij}, $i \neq j$, und $a_{ii} - a_{jj}$, $1 \leqq i, j \leqq n$, erzeugten Ideal. Die Ordnung $o(G)$ einer Untergruppe G von $GL(n,L)$ wird erzeugt von den Ordnungen $o(\sigma)$, $\sigma \in G$.

1.2. Sei J ein Ideal in L. Unter der *allgemeinen Kongruenzuntergruppe mod J von $GL(n,L)$, $GC(n,L,J)$*, verstehen wir die Gruppe

$$GC(n,L,J) = h_J^{-1}(\text{Zentrum } GL(n,L/J)). \tag{4}$$

Offenbar ist $GC(n,L,J)$ eine invariante Untergruppe von $GL(n,L)$ der Ordnung J. Insbesondere haben wir $GC(n,L,L) = GL(n,L)$ und $GC(n,L,0) =$ Zentrum $GL(n,L)$ isomorph L^*. Hier bezeichnet 0 das 0-Ideal in L.

Sei J ein Ideal in L. Unter der *speziellen Kongruenzuntergruppe mod J von $GL(n,L)$, $SC(n,L,J)$*, verstehen wir diejenige invariante Untergruppe von $GL(n,L)$, die erzeugt wird von den Transvektionen der Ordnung $\subset J$, d. h., von den Transvektionen in $GC(n,L,J)$. Eine *Transvektion* τ ist dabei ein Element aus $GL(n,L)$, für das es einen Unterraum H der Kodimension 1 (kurz: Hyperebene) in V gibt so, dass $\tau_{|H} =$ Identität und so, dass $\tau X - X \in H$ für alle $X \in V$.

Offenbar ist $SC(n,L,J)$ eine invariante Untergruppe von $GL(n,L)$ mit einer Ordnung $\subset J$, die in $GC(n,L,J)$ enthalten ist. Insbesondere ist $SC(n,L,0) = E =$ Einheitsgruppe. Für $SC(n,L,L)$ schreiben wir auch $SL(n,L)$ und nennen diese Gruppe die *spezielle lineare Gruppe in n Variablen über L.*

1.3. LEMMA. *Zwei Vektoren A und B von $V = V_n(L)$ haben dann und nur dann dieselbe Ordnung $o(A) = o(B)$, wenn es ein Element $\sigma \in GL(n,L)$ gibt so, dass $\sigma A = B$.*

Hieraus folgt

SATZ 1. *Zwei Transvektionen τ_1, τ_2 aus $GL(n,L)$ von derselben Ordnung $o(\tau_1) = o(\tau_2)$ sind konjugiert in $GL(n,L)$.*

ERGÄNZUNG. *Falls $n \geqq 3$ und $o(\tau_1) = o(\tau_2)$ ein Hauptideal ist, so sind τ_1 und τ_2 schon konjugiert in $SL(n,L)$.*

1.4. Hiermit lassen sich die speziellen Kongruenzuntergruppen folgendermassen charakterisieren:

THEOREM 1. *Sei J ein Ideal in dem lokalen Ring L und sei G eine Untergruppe von $GL(n,L)$. Folgende Aussagen sind äquivalent:*

(a) $G = SC(n,L,J)$.

(b) G *besteht aus den Elementen* $\sigma \in GL(n,L)$ *mit* $\det \sigma = 1$ *und* $h_J \sigma =$ *Identität.*

(c) $G =$ *gemischte Kommutatorgruppe* $\mathrm{Komm}(GL(n,L), GC(n,L,J))$. *Für* $n = 2$ *wird hierbei* $L/I \neq \mathbf{F}_2$ *vorausgesetzt.*

KOROLLAR. *Sei* G *eine Untergruppe von* $GL(n,L)$. *Folgende Aussagen sind äquivalent:*

(a) $G = SL(n,L)$.

(b) G *besteht aus den Elementen* $\sigma \in GL(n,L)$ *mit* $\det \sigma = 1$.

(c) G *ist die Kommutatorgruppe von* $GL(n,L)$. *Hier wird für* $n = 2$ *vorausgesetzt:* $L \neq \mathbf{F}_2$.

1.5. THEOREM 2. *Sei* J *ein Ideal in dem lokalen Ring* J.

(i) $GC(n,L,J)/SC(n,L,J)$ *ist isomorph zu der Untergruppe* $U(n,L,J)$ *von* $L^* \times (L/J)^*$, *die gebildet wird von den Elementen* $(a,b) \in L^* \times (L/J)^*$ *mit* $g_J a = b^n$.

(ii) *Setze* $HC(n,L,J) = GC(n,L,J) \cap SL(n,L)$. *Dann ist*

$$HC(n,L,J)/SC(n,L,J)$$

isomorph zur Gruppe $E_n((L/J)^*)$ *der* n*-ten Einheitswurzeln in* $(L/J)^*$.

KOROLLAR. $GL(n,L)/SL(n,L)$ *ist isomorph zu* L^*. *Zentrum* $GL(n,L)$ *ist isomorph zu* L^*. *Zentrum* $SL(n,L)$ *ist isomorph zu* $E_n(L^*)$.

1.6. $GC(n,L,J)$ und $SC(n,L,J)$ sind invariante Untergruppen der Ordnung J. Nach Theorem 2 ist $GC(n,L,J)/SC(n,L,J)$ kommutativ, also ist jede Untergruppe G von $GL(n,L)$, die der Beziehung

$$GC(n,L,J) \supset G \supset SC(n,L,J) \tag{5}$$

genügt, eine invariante Untergruppe der Ordnung $o(G) \subset J$.

Das Hauptergebnis der vorliegenden Arbeit ist nun, dass umgekehrt jede invariante Untergruppe G der Ordnung $o(G) = J$ der Beziehung (5) genügt. Wir werden sogar allgemeiner beweisen, dass dies für die unter $SL(n,L)$ invarianten Untergruppen G von $GL(n,L)$ gilt.

Zunächst beweisen wir

SATZ 2. *Sei* $(\tau_\alpha)_{\alpha \in A}$ *eine Menge von Transvektionen* τ_α *der Ordnung* $o(\tau_\alpha) = J_\alpha$. *Die von den* τ_α *erzeugte, unter* $SL(n,L)$ *invariante Untergruppe*

G in $GL(n,L)$ ist gleich $SC(n,L,J)$, wo J das von den J_α, $\alpha \in A$, erzeugte Ideal in L ist. Für $n=2$ setzen wir voraus: $\operatorname{char}(L/I) \neq 2$.

Sodann beweisen wir den fundamentalen

SATZ 3. *Sei G eine unter $SL(n,L)$ invariante Untergruppe von $GL(n,L)$ der Ordnung $o(G)=J$. Dann enthält G die Gruppe $SC(n,L,J)$. Hier setzen wir für $n=2$ voraus:* $\operatorname{char}(L/I) \neq 2$ *und* $L/I \neq F_3$.

1.7. Durch Zusammenfassung der vorstehenden Ergebnisse erhalten wir den folgenden Satz über die Struktur der allgemeinen und der speziellen linearen Gruppe über einem lokalen Ring L:

THEOREM 3. *Sei L ein lokaler Ring.*

(i) *Eine Untergruppe G von $GL(n,L)$, die invariant ist unter $SL(n,L)$, bestimmt ein Ideal J von L so, dass* (5) *gilt. Umgekehrt ist jede Untergruppe G von $GL(n,L)$, die den Beziehungen* (5) *genügt, eine invariante Untergruppe von $GL(n,L)$ der Ordnung $o(G)=J$.*

(ii) *Eine invariante Untergruppe G von $SL(n,L)$ bestimmt ein Ideal J von L so, dass*

$$HC(n,L,J) = GC(n,L,J) \cap SL(n,L) \supset G \supset SC(n,L,J) \tag{6}$$

gilt. Umgekehrt ist jede Untergruppe G von $SL(n,L)$, die den Beziehungen (6) *genügt, invariant und von der Ordnung J.*

Für $n=2$ setzen wir voraus: $\operatorname{char}(L/I) \neq 2$ *und* $L/I \neq F_3$.

KOROLLAR. (Dieudonné [4], [5]) *Sei L ein kommutativer Körper.*

(i) *Für eine Untergruppe G von $GL(n,L)$, die invariant ist unter $SL(n,L)$, gilt eine folgenden Beziehungen:*

$$\begin{gathered} GL(n,L) \supset G \supset SL(n,L), \\ \text{Zentrum}\, GL(n,L) \supset G \supset E. \end{gathered} \tag{7}$$

Umgekehrt ist jede Untergruppe G von $GL(n,L)$, die einer der Beziehungen (7) *genügt, invariant in $GL(n,L)$.*

(ii) *Die invarianten Untergruppen G von $SL(n,L)$, $G \neq SL(n,L)$, gehören zu* $(\text{Zentrum}\, GL(n,L)) \cap SL(n,L) = \text{Zentrum}\, SL(n,L)$.

Hier setzen wir für $n=2$ voraus: $\operatorname{char} L \neq 2$ *und* $L \neq F_3$.

1.8. Wir können auf Grund von Theorem 2 und 3 folgendes feststellen:

(a) Die unter $SL(n,L)$ invarianten Untergruppen G von $GL(n,L)$ der Ordnung J genügen den Bedingungen (5), das heisst, $GC(n,L,J)$ und $SC(n,L,J)$ sind die grösste bzw. die kleinste unter $SL(n,L)$ invariante Untergruppe der Ordnung J in $GL(n,L)$, und jede zwischen diesen beiden Gruppen gelegene Gruppe G ist invariant in $GL(n,L)$ und von der Ordnung J.

(b) Jede unter $SL(n,L)$ invariante Untergruppe G von $GL(n,L)$ (die dann auch invariant ist unter $GL(n,L)$) ist bestimmt durch ihre Ordnung $o(G)=J$ und durch die Gruppe $G/SC(n,L,J)$, die eine Untergruppe der in Theorem 2 eingeführten kommutativen Gruppe $U(n,L,J)$ ist.

Das Entsprechende gilt für die invarianten Untergruppen von $SL(n,L)$.

1.9. Für den Fall $L=\mathbf{Z}/(p^r)$, p eine Primzahl, sind die vorstehenden Ergebnisse bewiesen von Brenner [2].

Für den Fall, dass L ein verallgemeinerter Bewertungsring ist, das heisst, ein kommutativer Ring mit Eins, für den die Ideale total geordnet sind, sind vorstehende Ergebnisse bewiesen in [7].

Wie schon in [7], schliessen wir uns in den Bezeichnungen und den Anordnungen der Beweise der Darstellung an, die Artin [1] von der Theorie der linearen Gruppen gegeben hat.

1.10. Die vorstehenden Ergebnisse bleiben im wesentlichen gültig, wenn man *lineare Gruppen $GL(n,L)$ über nichtkommutativen lokalen Ringen L* betrachtet. Ein nichtkommutativer lokaler Ring ist, nach Cartan-Eilenberg [3], ein nichtkommutativer Ring L mit Eins und einem grössten Ideal I; I ist zweiseitiges Ideal; L/I est ein nicht notwendig kommutativer Körper. Wir wollen ferner voraussetzen, dass jedes Linksideal J von L auch Rechtsideal ist. Die Klasse dieser Ringe unfasst, für $I=0$, die nichtkommutativen Körper.

Die im folgenden geführten Beweise bleiben, jedenfalls für $n\geqq 3$, auch für die linearen Gruppen $GL(n,L)$ über einem solchen nichtkommutativen lokalen Ring gültig; nur beim Beweis der Beziehung:

$$SC(n,L,J)=\mathrm{Komm}(GL(n,L),GC(n,L,J)),$$

Theorem 1(c), sind einige zusätzliche Überlegungen nötig, die damit zusammenhängen, dass man in Theorem 1(b) den Begriff der Determinante verfeinern muss. Und zwar tritt an die Stelle der gewöhnlichen Determinante eine für jedes Ideal J von L erklärte J-Determinante:

$$\det_J\colon GC(n,L,J)\to \bar{L}(J,n)$$

wobei $\bar{L}(J,n) = g_J^{-1}(\mathrm{Zentrum}(L/J)^*)^n/\mathrm{Komm}(L^*, g_J^{-1}\,\mathrm{Zentrum}(L/J)^*)$ eine Untergruppe von $L^*/\mathrm{Komm}(L^*)$ ist. Für $J = L$ stimmt $\det_J$ überein mit der von Dieudonné [4], [5] eingeführten Determinante über nichtkommutativen Körpern.

In Theorem 2 ist entsprechend zu lesen: $GC(n,L,J)/SC(n,L,J)$ ist isomorph zu der Untergruppe der Paare (a,b) in $\bar{L}(J,n) \times \mathrm{Zentrum}(L/J)^*$ mit $g_J a = b^n$. Speziell für $J = L$ and $J = 0$ liefert dies: $GL(n,L)/SL(n,L)$ ist isomorph zu $L^*/\mathrm{Komm}\,L^*$, Zentrum $GL(n,L)$ ist isomorph zu Zentrum L^*.

Als Korollar erhält man die Sätze von Dieudonné [4], [5] über die Struktur der linearen Gruppen über nichtkommutativen Körpen.

Die vollständigen Beweise dieser Verallgemeinerung sollen anderweitig veröffentlicht werden.

2. Beweise.

2.1. *Beweis des Lemmas.* Falls es ein $\sigma \in GL(n,L)$ gibt mit $\sigma A = B$, dann ist $g_J A = 0$ äquivalent mit $g_J B = g_J \sigma A = h_J \sigma g_J A = 0$, also $o(A) = o(\sigma A) = o(B)$.

Sei nun umgekehrt $o(A) = o(B) = J$. Bezüglich einer Basis E_i, $1 \leqq i \leqq n$, sei $A = \sum E_i a_i$. J wird erzeugt von den a_i. Sei u_α, $1 \leqq \alpha \leqq p \leqq n$, eine minimale Anzahl von erzeugenden Elementen von J. Dann ist also $u_\alpha = \sum r_{\alpha j} a_j$ und $a_i = \sum b_{i\beta} u_\beta$ und $u_\alpha = \sum r_{\alpha j} b_{j\beta} u_\beta$, das heisst $\sum(\sum r_{\alpha j} b_{j\beta} - \delta_{\alpha\beta}) u_\beta = 0$. Da die u_α ein minimales System von Erzeugenden bilden, kann keines der Elemente $\sum r_{\alpha j} b_{j\beta} - \delta_{\alpha\beta}$ zu L^* gehören, mit anderen Worten, $\sum r_{\alpha j} b_{j\beta} - \delta_{\alpha\beta} = 0 \bmod I$.

Wir setzen $F_\alpha = \sum E_j b_{j\alpha}$ und behaupten, dass die F_α linear unabhängig sind $\bmod I$. In der Tat, aus $\sum F_\beta c_\beta = \sum E_j b_{j\beta} c_\beta = 0 \bmod I$ folgt $\sum b_{j\beta} c_\beta = 0 \bmod I$ und also $\sum r_{\alpha j} b_{j\beta} c_\beta = c_\alpha = 0 \bmod I$. Die F_α können zu einer Basis F_i ergänzt werden. Denn sei E_i, $1 \leqq i \leqq n$, eine Basis von V und $F_\alpha = \sum E_i f_{i\alpha}$. Die (n,p)-Matrix $(f_{i\alpha})$, $1 \leqq i \leqq n$, $1 \leqq \alpha \leqq p$, hat $\bmod I$ den Rang p, sie lässt sich also $\bmod I$ zu einer (n,n)-Matrix vom Rang n erweitern. Wenn dann (f_{ij}), $1 \leqq i, j \leqq n$, ein Urbild einer solchen Erweiterung ist, so setze man $F_j = \sum E_i f_{ij}$. Offenbar ist $A = \sum F_\alpha u_\alpha$.

Da $o(B) = o(A) = J$, können wir auch B in der Form $B = \sum G_\alpha u_\alpha$ schreiben, wo die G_α linear unabhängig sind $\bmod I$. Die G_α können also zu einer Basis G_i ergänzt werden. Wir erklären $\sigma \in GL(n,L)$ durch $\sigma F_i = G_i$. Dann wird $\sigma A = B$.

2.2. *Beweis von Satz* 1. Sei τ eine Transvektion, H eine Hyperebene mit $\tau|_H =$ Identität. Sei ϕ eine Linearform mit $\phi^{-1}(0) = H$. Sei B ein

Vektor mit $\phi(B)=1$. Dann ist $X-B\phi(X)\in H$ für alle $X\in V$ und daher $\tau X-\tau B\phi(X)=X-B\phi(X)$. Wir setzen $A=\tau B-B\in H$. Damit wird

$$\tau X=X+A\phi(X). \tag{8}$$

Wir sagen: *Der Vektor* A *in* (8) *gehört zu der Transvektion* τ. A ist durch τ (oder genauer: durch H) nur bis auf ein Element $c\in L^*$ bestimmt; denn wenn ϕ ersetzt durch $c\phi$, dann geht A über in Ac^{-1}. Offenbar ist $o(\tau)=o(A)$, wenn A zu τ gehört.

Wir machen jetzt die Voraussetzungen von Satz 1. τ_1 und τ_2 stellen wir dar durch

$$\tau_r X=X+A_r\phi_r(X) \qquad (r=1,2). \tag{9}$$

B_r sei so gewählt dass $\phi_r(B_r)=1$. Da $o(\tau_1)=o(\tau_2)$, ist $o(A_1)=o(A_2)$. Nach dem Lemma gibt es also ein $\sigma\in GL(n,L)$ mit $\sigma A_1=A_2$. Aus dem Lemma für $n-1$ folgt, dass man zugleich $\sigma H_1=H_2$ erreichen kann, wo $H_r=\phi_r^{-1}(0)$, und dann kann man noch erreichen $\sigma B_1=B_2$. Dann ist jedoch $\tau_2=\sigma\tau_1\sigma^{-1}$. Die Ergänzung zu Satz 1 beweisen wir in 2.4.

2.3. *Beweis von Theorem* 1.

2.3.1. Wir bezeichnen die durch (b) definierte Gruppe mit H_J und die durch (c) definierte Gruppe mit K_J.

2.3.2. Offenbar gilt für jede Transvektion τ mit $o(\tau)\subset J$: $\det\tau=1$ und $h_J\tau=$ Identität, also $SC(n,L,J)\subset H_J$.

Sei nun umgekehrt σ ein Element aus H_J. Falls $J=L$, das heisst, falls $SC(n,L,J)=SL(n,L)$, dann kann man bekanntlich (vgl. Dieudonné l. c. oder Artin l. c.) eine Matrixdarstellung von σ durch Multiplikation mit geeigneten Elementen von $SL(n,L)$ von rechts und von links auf die Form $\operatorname{diag}(1,1,\cdots,a)$ bringen, wo $a=\det\sigma=1$ ist.

Sei jetzt $\sigma\in H_J$ mit $J\subset I$. Sei σ dargestellt durch die Matrix $((a_{ik}))$. Da $h_J\sigma=$ Identität, ist $a_{ik}\in J$ für $i\neq k$ und $a_{ii}-1\in J$. Indem wir von links und von rechts mit geeigneten Elementen aus $SC(n,L,J)$ multiplizieren, können wir $((a_{ik}))$ auf die Gestalt $\operatorname{diag}(1+u_1,1+u_2,\cdots,1+u_n)$, $u_i\in J$, bringen.

Die Formel

$$\begin{pmatrix}1 & -(1+u)^{-1}u\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ u(1+u)^{-1} & 1\end{pmatrix} = \begin{pmatrix}(1+u)^{-1} & 0\\ 0 & 1+u\end{pmatrix} \tag{10}$$

zeigt, dass auch das Element $\operatorname{diag}((1+u)^{-1}, 1, \cdots, 1+u)$, $u \in J$, zu $SC(n, L, J)$ gehört. Daher können wir durch Multiplikation mit geeigneten Elementen von $SC(n, L, J)$ aus $((a_{ik}))$ sogar die Matrix $\operatorname{diag}(1, 1, \cdots, 1+w)$, $w \in J$, erhalten. Wegen $\det((a_{ik})) = \det \operatorname{diag}(1, 1, \cdots, 1+w) = 1 + w = 1$ ist $w = 0$, also $\sigma \in SC(n, L, J)$, d. h. $H_J \subset SC(n, L, J)$.

2. 3. 3. Ein erzeugendes Element von K_J hat die Gestalt $\rho\sigma\rho^{-1}\sigma^{-1}$ mit $\rho \in GL(n, L)$ und $\sigma \in GC(n, L, J)$. Da $h_J\sigma \in$ Zentrum $GL(n, L/J)$, ist $h_J\rho\sigma\rho^{-1}\sigma^{-1} = h_J\rho h_J\sigma h_J\rho^{-1} h_J\sigma^{-1} =$ Indentität. Da ferner $\det \rho\sigma\rho^{-1}\sigma^{-1} = 1$, haben wir $K_J \subset H_J = SC(n, L, J)$.

Sei nun umgekehrt τ eine Transvektion aus $SC(n, L, J)$. Wir schreiben τ in der Form (8) mit $A \in \phi^{-1}(0) = H$. Wir betrachten zunächst den Fall $n \geqq 3$. Dann ist also $\dim H \geqq 2$. Wir behaupten, dass wir dann A in der Form $A = A_2 - A_1$ schreiben können mit $o(A_1) = o(A_2) = o(A)$ und $A_1 \in H$, $A_2 \in H$.

In der Tat, es sei $A = \sum E_i a_i$, wo E_i, $1 \leqq i \leqq n-1$, eine Basis für H ist. Falls $n - 1 = 2m$, so setzen wir

$$A_1 = \sum E_{2j-1}(a_{2j} - a_{2j-1}) + \sum E_{2j} a_{2j-1},$$

$$A_2 = \sum E_{2j-1} a_{2j} + \sum E_{2j}(a_{2j-1} + a_{2j}) \qquad (j = 1, \cdots, m).$$

Falls $n - 1 = 2m + 1$, so ersetzen wir in den vorstehenden Ausdrücken den Summanden $j = 1$ durch

$$E_1(a_{2m+1} + a_2 - a_1) + E_2(a_1 + a_{2m+1}) + E_{2m+1} a_1,$$

$$E_1(a_2 + a_{2m+1}) + E_2(a_1 + a_2 + a_{2m+1}) + E_{2m+1}(a_{2m+1} + a_1).$$

Wir definieren nun τ_r $(r = 1, 2)$ durch (9) mit $\phi_r = \phi$. Nach Satz 1 gibt es $\sigma \in GL(n, L)$ mit $\tau_2 = \sigma\tau_1\sigma^{-1}$. Also

$$\tau = \tau_2\tau_1^{-1} = \sigma\tau_1\sigma^{-1}\tau_1^{-1} \in K_J, \text{ d. h. } SC(n, L, J) \subset K_J.$$

Im Falle $n = 2$ benutzen wir die Voraussetzung dass $L/I \neq F_2$. Es gibt dann ein $c \in L^*$ so, dass $A = A_2 - A_1$, $A_2 = A(1 + c)$, $A_1 = Ac$, $o(A) = o(A_1) = o(A_2)$. Nach Satz 1 gibt es ein $\sigma \in GL(2, L)$ so, dass $\tau = \sigma\tau_1\sigma^{-1}\tau_1^{-1} \in K_J$, also $SC(2, L, J) \subset K_J$.

2. 4. *Beweis von Satz* 1, *Ergänzung*. Wir verwenden die Bezeichnungen aus 2. 2. Insbesondere ist also τ_r $(r = 1, 2)$ dargestellt durch (9). Sei $H_r = \phi_r^{-1}(0)$. Nach Voraussetzung ist $o(\tau_r) = o(A_r) = (a)$ ein Hauptideal. Das heisst, wir können A_r in der Form $A_r = E_r a$, $o(E_r) = L$, schreiben. Da $n \geqq 3$, also $\dim H_r = n - 1 \geqq 2$, gibt es in H_r einen Vektor F_r, der linear

unabhängig mod I von E_r ist, $r = 1, 2$. Wir ergänzen E_1, F_1 zu einer Basis von H_1 und ergänzen, für ein beliebiges $c \in L^*$, $E_2, F_2 c$ zu einer Basis von H_2. Damit erkennen wir, dass es stets $\sigma \in GL(n,L)$ so gibt, dass $\sigma E_1 = E_2$ (also $\sigma A_1 = A_2$), $\sigma F_1 = F_2 c$ und $\sigma H_1 = H_2$, $\sigma B_1 = B_2$, also $\tau_2 = \sigma \tau_1 \sigma^{-1}$. Wenn wir $c \in L^*$ geeignet wählen, können wir erreichen, dass $\det \sigma = 1$, das heisst, $\sigma \in SL(n,L)$.

2.5. *Beweis von Theorem* 2. Wir betrachten den Homomorphismus

$$f\colon \sigma \in GC(n,L,J) \to (\det \sigma, h_J \sigma) \in L^* \times \text{Zentrum } GL(n, L/J).$$

Die rechts stehende Gruppe ist isomorph $L^* \times (L/J)^*$. Nach Theorem 1 ist $\operatorname{Kern}(f) = SC(n,L,J)$.

Sei $\sigma \in GC(n,L,J)$ und $\det \sigma = a \in L^*$. Dann ist

$$g_J a = g_J \det \sigma = \det h_J \sigma = \det \operatorname{diag}(b, b, \cdots, b) = b^n, \quad b \in (L/J)^*.$$

Zu einem $b \in (L/J)^*$ wähle man ein $b' \in L^*$ mit $g_J b' = b$. Dann stellt die Matrix $((b' \delta_{ik}))$ ein Element σ aus $GC(n,L,J)$ dar mit $g_J \det \sigma = b^n$.

2.6. *Beweis von Satz* 2.

2.6.1. Wir betrachten zunächst den Fall $n \geqq 3$ und nehmen an, das die Menge $(\tau_\alpha)_{\alpha \in A}$ aus einem einzigen Element τ besteht. τ sei dargestellt durch (8) mit $A = \sum E_i a_i$, $1 \leqq i \leqq n-1$, wobei die Vektoren E_i, $1 \leqq i \leqq n-1$, eine Basis für die Hyperebene $H = \phi^{-1}(0)$ bilden. $J = o(\tau) = o(A)$ wird erzeugt von den Elementen a_i, $1 \leqq i \leqq n-1$.

Wir definieren A_1 und A_2 durch

$$A_1 = \sum_1^{n-1} E_i a_i - \sum_2^{n-1} E_i a_{i-1}; \qquad A_2 = \sum_2^{n-1} E_i a_{i-1}.$$

Wir haben $A_2 = A - A_1$ und $o(A) = o(A_1)$. Wir erklären die Transvektionen τ_r $(r = 1, 2)$ durch (9). Nach Satz 1 gibt es $\sigma \in GL(n,L)$ mit $\tau_1 = \sigma \tau \sigma^{-1}$. Da man speziell σ so wählen kann, dass $\sigma E_i = E_i - E_{i+1}$ $(i < n-1)$, $\sigma E_{n-1} = E_{n-1}$, erkennt man, dass es sogar in $SL(n,L)$ ein σ gibt mit $\tau_1 = \sigma \tau \sigma^{-1}$, d. h. $\tau_1 \in G =$ die von τ erzeugte unter $SL(n,L)$ invarianten Untergruppe von $GL(n,L)$. Dann auch $\tau_2 = \tau \tau_1^{-1} \in G$, und indem wir auf τ_2 einen entsprechenden Schluss anwerden erkennen wir, dass G eine Transvektion enthält mit zugehörigem Vektor $E_{n-1} a_1$.

Auf Grund der Ergänzung zu Satz 1 können wir sagen, dass G alle Transvektionen enthält mit zugehörigem Vektor $E a_1 c \, (= (Ec) a_1)$, wo $o(E) = L$ und $c \in L^*$. Offenbar ergibt sich genau so, dass G auch die Transvektionen mit zugehörigem Vektor Ea_ic, $1 \leqq i \leqq n-1$, $o(E) = L$, $c \in L^*$, enthält. Wenn $c \in I$, so $c-1 \in L^*$. Da $Ea_ic = Ea_i(c-1) + Ea_i$, enthält G auch die Transvektionen mit Vektor Ea_ic, $o(E) = L$, $c \in L$, und durch Produktbildung folgt: G enthält alle Transvektionen mit Vektor Eb, wo $b = \sum a_ic_i$ ein beliebiges Element aus dem Ideal $J = o(\tau)$ ist.

Sei schliesslich τ' eine beliebige Transvektion der Ordnung $o(\tau') = J' \subset o(\tau) = J$.

$$\tau'X = X + A'\phi'(X) \tag{11}$$

sei eine Darstellung von τ'. Wir schreiben $A' = \sum E'_ia'_i$, $1 \leqq i \leqq n-1$, wobei die E'_i, $1 \leqq i \leqq n-1$, eine Basis von $H' = \phi'^{-1}(0)$ bilden. Wegen $a'_i \in J$ gehören die Transvektionen

$$\tau'_iX = X + E'_ia'_i\phi'(X) \tag{12}$$

zu G, also auch $\tau' = \prod \tau'_i \in G$.

2.6.2. Wir betrachen jetzt den Fall $n \geqq 3$ mit einer beliebigen Menge $(\tau_\alpha)_{\alpha\in A}$. Sei J das von den $J_\alpha = o(\tau_\alpha)$ erzeugte Ideal. Eine beliebige Transvektion τ' mit $o(\tau') = J' \subset J$ besitzt eine Darstellung (11) mit $A' = \sum E'_ia'_i$, $1 \leqq i \leqq n-1$, $a'_i \in J' \subset J$. Die Überlegungen aus 2.6.1 zeigen, dass G die Transvektionen τ'_i, $1 \leqq i \leqq n-1$, der Form (12) enthält, also auch $\tau' = \prod \tau'_i \in G$.

2.6.3. Wir betrachten den Fall $n = 2$ und nehmen zunächst wiederum an, dass die Menge $(\tau_\alpha)_{\alpha\in A}$ nur aus dem Element τ besteht. Durch geeignete Wahl der Basis lässt such τ in der Form

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \tag{13}$$

darstellen, wo $(u) = o(\tau)$ ist. Dann repräsentiert auch

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & ua^2 \\ 0 & 1 \end{pmatrix}, \qquad a \in L^*, \tag{14}$$

ein Element aus der von τ erzeugten, unter $SL(2, L)$ invarianten Gruppe G. Mit der Matrix (13) enthält G also auch die Matrizen

$$\begin{pmatrix} 1 & u(\sum \pm a_i^2) \\ 0 & 1 \end{pmatrix}, \qquad a_i \in L^*. \tag{15}$$

Da $2 \in L^*$, haben wir für jedes $c \in L$ die Darstellung

$$c = (c+1)^2/2^2 - (c-1)^2/2^2. \tag{16}$$

Falls also $c+1 \in L^*$ und $c-1 \in L^*$, so haben wir aus (15) und (16), dass G auch die Matrix

$$\begin{pmatrix} 1 & uc \\ 0 & 1 \end{pmatrix} \tag{17}$$

enthält. Falls dagegen $c+1 \in I$ oder $c-1 \in I$, so ersetzen wir c zunächst durch $c' = c+1$ beziehungsweise durch $c' = c-1$. Dann ist $c'+1 \in L^*$ und $c'-1 \in L^*$ und auf Grund von (15) und (16) enthält G also eine Matrix (17), in der c durch c' ersetzt ist. Da auch (13) zu G gehört, folgt, dass auch (17) zu G gehört.

Da ein 1-dimensionaler Unterraum von $V = V_2(L)$ in einen anderen 1-dimensionalen Unterraum von V stets durch ein Element $\sigma \in SL(2, L)$ übergeführt werden kann, folgt, dass G mit der Transvektion τ, (13), der Ordnung $o(\tau) = (u)$ auch alle Transvektionen τ' der Ordnung $o(\tau') \subset o(\tau) = (u)$ enthält.

Wir betrachten jetzt eine beliebige Menge $(\tau_\alpha)_{\alpha \in A}$ von Transvektionen τ_α. Sei J das von den $J_\alpha = o(\tau_\alpha) = (u_\alpha)$ erzeugte Ideal. Eine beliebige Transvektion τ' der Ordnung $o(\tau') = (u') \subset J$ lässt sich darstellen durch (13) mit u' statt u. u' lässt sich schreiben als $u' = \sum u_\alpha c_\alpha$, $c_\alpha = 0$ für fast alle $\alpha \in A$. Die von den τ_α erzeugte, unter $SL(2, L)$ invariante Untergruppe G von $GL(2, L)$ enthält, wie wir soeben sahen, alle Transvektionen (17) mit $u_\alpha c_\alpha$ an Stelle von uc. Also gehört auch das Produkt dieser Transvektionen zu G, d. h. $\tau' \in G$.

2.7. *Beweis von Satz 3 für $n = 2$.*

2.7.1. Angenommen, G enthält das Element ρ der Form $\begin{pmatrix} a & u \\ 0 & a+v \end{pmatrix}$ mit $(v) = K$. $\left(\begin{matrix} 1 & -a-v \\ 0 & 1 \end{matrix}\right.$; Transvektion τ. Dann gehört auch $\rho\tau\rho^{-1}\tau^{-1}$: $\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$ zu G, das heisst, G enthält eine Transvektion der Ordnung $(v) = K$ und daher, nach Satz 2, $SC(n, L, K) \subset G$.

2.7.2. Wir betrachten den Fall, das $o(G) = J \subset I$. Ein Element $\sigma \in G$ besitzt die Darstellung

$$\begin{pmatrix} b & x \\ y & b+z \end{pmatrix} \tag{18}$$

mit $x, y, z \in J = o(G)$, $b \in L^*$. Es ist $o(\sigma) = (x, y, z) =$ das von x, y und z erzeugte Ideal in L. Wenn wir zeigen, dass G mit σ, (18), auch die Transvektionen

$$\begin{pmatrix} 1 & y-x \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & y-2x \mp z \\ 0 & 1 \end{pmatrix} \tag{19}$$

enthält, deren Ordnungen offenbar gerade das Ideal $o(\sigma)$ erzeugen, dann haben wir auf Grund von Satz 2, dass $SC(2, L, o(\sigma)) \subset G$. Da dies für jedes $\sigma \in G$ gilt, folgt $SC(2, L, J) \subset G$.

Wir beweisen die Existenz der Transvektionen (19) in zwei Schritten.

2.7.2.1. Da G invariant ist unter $SL(2, L)$, enthält G mit σ, (18), auch das Element

$$(20)\qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b & x \\ y & b+z \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} b & x \\ y & b+z \end{pmatrix}$$
$$= \begin{pmatrix} b^2+bz-y^2 & bx+xz-by-yz \\ -bx+by & b^2+bz-x^2 \end{pmatrix} = (\text{kurz}) \begin{pmatrix} b' & x' \\ y' & b'+z' \end{pmatrix}.$$

Dann gehört auch σ'':

$$(21)\qquad \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} b' & x' \\ y' & b'+z' \end{pmatrix}\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b'+ky' & -k^2y'+x'+kz' \\ y' & b'-ky'+z' \end{pmatrix}$$

zu G. Wenn wir in (21) setzen: $k = (x+y)/2b$, so erhalten wir für $\sigma'' \in G$ die Darstellung

$$(22)\qquad \begin{pmatrix} b^2+bz-(y^2+x^2)/2 & (y^2-x^2)(y+x)/4b-(b+z)(y-x) \\ b(y-x) & b^2+bz-(y^2+x^2)/2 \end{pmatrix}$$
$$= (\text{kurz}) \begin{pmatrix} a & u \\ v & a \end{pmatrix}.$$

Das Element $\tau \in SL(2, L)$ sei erklärt durch $\begin{pmatrix} 1+v & -a(1+v)^{-1}(2+v) \\ 0 & (1+v)^{-1} \end{pmatrix}$. Dann gehört auch $\rho' = \tau^{-1}\sigma''^{-1}\tau\sigma''$ zu G. Wir finden für ρ':

$$(23)\qquad (a^2-uv)^{-1}\begin{pmatrix} a^2-a^2v(2+v)-uv(1+v)^{-2} & \cdots \\ 0 & a^2-a^2v(2+v)-uv(1+v)^2 \end{pmatrix}$$
$$= (\text{kurz}) \begin{pmatrix} a' & u' \\ 0 & a'+v' \end{pmatrix} \text{mit } (v') = (v) = (y-x).$$

Aus 2.7.1, angewandt auf das Element ρ', (23), folgt dass G die erste der Transvektionen (19) enthält.

2.7.2.2. Mit dem Element σ, (18), enthält G auch die Elemente

$$(24)\qquad \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix}\begin{pmatrix} b & x \\ y & b+z \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \mp 1 & 1 \end{pmatrix} = \begin{pmatrix} b \mp x & x \\ y-x \mp z & b \pm x + z \end{pmatrix}.$$

Indem wir auf die Elemente (24) dieselben Überlegungen anwenden, die wir auf das Element σ, (18), in 2.7.2.1 angewandt haben, erkennen wir, dass G auch die Transvektionen der Ordnung $(y - 2x \mp z)$ enthält, also die letzten beiden der Transvektionen (19).

2.7.3. Wir betrachten jetzt den Fall dass $o(G) = J = L$. Dann enthält G ein Element σ der Form

$$(25) \qquad \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}, \qquad a \in L^*.$$

Mit dem Element τ: $\begin{pmatrix} bd & d^{-1} \\ -d & 0 \end{pmatrix}$ aus $SL(2, L)$ gehört dann auch $\rho = \tau^{-1}\sigma^{-1}\tau\sigma$:

$$(26) \qquad \begin{pmatrix} -a^{-1}d^{-2} & -b - a^{-1}d^{-2}b \\ 0 & -ad^2 \end{pmatrix}$$

zu der Gruppe G. Um 2.7.1 anwenden zu können, müssen wir $d \in L^*$ so wählen, dass $a^{-1}d^{-2} - ad^2 \in L^*$, d.h.

$$(27) \qquad a^2d^4 - 1 \in L^*.$$

Da wir $\mathrm{char}(L/I) \neq 2$ und $L/I \neq \boldsymbol{F}_3$ vorausgesetzt haben, existiert ein $d \in L^*$ mit (27) stets dann, wenn $L/I \neq \boldsymbol{F}_5$ est, denn dann hat L/I wenigstens 6 Elemente. Wenn (27) gilt, dann folgt aus 2.7.1 mit ρ, (26), dass G eine Transvektion der Ordnung L enthält, also nach Satz 2, $SL(2, L) \subset G$.

2.7.3.1. Es bleibt also der Fall $L/I = \boldsymbol{F}_5$ zu betrachten. Falls $g_I a^2 \neq 1$ ist, dann gibt es ein $d \in L^*$ so, dass (27) gilt. Wir können uns also auf den Fall $g_I a = \pm 1$ beschränken.

Zunächst können wir dann $d \in L^*$ so wählen, dass $g_I ad^2 = 1$ ist. Neben dem Element ρ, (26), enthält G auch das Element ρ', das aus (26) entsteht, wenn man d ersetzt durch $a^{-1}d^{-1}$. Dann gehört auch $\rho\rho'$ zu G. $\rho\rho'$ hat die Form

$$(28) \qquad \begin{pmatrix} 1 & b(1 + a^{-1}d^{-2})^2 \\ 0 & 1 \end{pmatrix}.$$

$\rho\rho'$ ist also eine Transvektion der Ordnung (b). Falls $(b) = L$, so haben wir mit Satz 2 $SL(2, L, L) = SL(2, L) \subset G$. Falls $(b) \subset I$, so haben wir mit Satz 2 $SL(2, L, (b)) \subset G$. Dann gehört auch das Element

$$(29) \qquad \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$$

zu G.

Wir haben also jetzt ein Element σ, (25), mit $b = 0$ und $g_I a = \pm 1$ in G. Damit enthät G auch das Element ρ, (26), mit $d = 1$. Es ist also $o(\rho) = J' = (a^2 - 1) \subset I$. Nach 2.7.2 ist dann jedenfalls $SC(2, L, J') \subset G$.

Wir betrachten die Fälle: (i) $J' = (a - 1)$, (ii) $J' = (a + 1)$. Im Falle (i) wählen wir für das Element σ, (29), eine neue Basis so, dass σ die Darstellung erhält:

$$(30)\qquad \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & a\\ 1 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{1}{2} & -\frac{1}{2}\end{pmatrix}=\begin{pmatrix}(1+a)/2 & (1-a)/2\\ (-1+a)/2 & (-1-a)/2\end{pmatrix}.$$

Es ist also $h_{J'}\sigma\colon \begin{pmatrix}1 & 0\\ 0 & 1-2\end{pmatrix}$. Aus 2.7.1 folgt, dass $SL(2, L/J') \subset h_{J'}G$.

Im Falle (ii) wählen wir für σ, (29), eine Basis wie folgt:

$$(31)\qquad \begin{pmatrix}1 & 2\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & a\\ 1 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{1}{4} & -\frac{1}{4}\end{pmatrix}=\begin{pmatrix}(4+a)/4 & (4-a)/4\\ (-4+a)/4 & (-4-a)/4\end{pmatrix}.$$

Es ist also $h_{J'}\sigma\colon \begin{pmatrix}2 & 0\\ 0 & 2-4\end{pmatrix}$. Aus 2.7.1 folgt wiederum $SL(2, L/J') \subset h_{J'}G$. Da $\operatorname{Kern}(h_{J'} \mid_{SL(n,L)}) = SC(n, L, J') \subset G$, folgt $SL(2, L) \subset G$.

2.8. *Beweis von Satz 3 für $n \geqq 3$.*

2.8.1. Angenommen, G enthält ein Element ρ so, dass $\rho X - X \in H$ für alle $X \in V$, wo H ein Unterraum der Kodimension 1 ist. Behauptung: Dann enthält G auch die Transvektion τ der Form

$$(32)\qquad \tau X = X + (\rho U - U)\phi(X)$$

wo $\phi^{-1}(0) = H$ und U ein beliebiger Vektor H ist. In der Tat, setze $\tau' X = X + U\phi(X)$. Dann gehört auch $\tau = \rho\tau'\rho^{-1}\tau'^{-1}$ zu G. Wegen $\phi(\rho X) = \phi(X)$ und $\phi(\rho^{-1}U) = \phi(\rho U) = 0$ hat τ die Gestalt (32).

2.8.2. Sei $\sigma \in G$. Das Ideal $o(\sigma) \subset J = o(G)$ wird erzeugt von Elementen $a \in L$, deren jedes in folgender Weise beschrieben werden kann: Es gibt einen Vektor E der Ordnung $o(E) = L$ und eine Linearform ϕ der Ordnung L so, dass $\phi(E) = 0$ und $\phi(\sigma E) = a$. Wenn wir zeigen, wass, für jedes solche a, G eine Transvektion der Ordnung (a) enthält, dann ist der Satz 3 bewiesen.

Denn jedenfalls enthält G dann, auf Grund von Satz 2, die Gruppen $SC(n, L, o(\sigma))$ für jedes $\sigma \in G$, und da $J = o(G)$ erzeugt wird von $o(\sigma)$, $\sigma \in G$, folgt die Behauptung mit Satz 2.

2.8.3. Sei $\sigma \in G(n, L)$. Sei E ein Vektor der Ordnung L und ϕ eine Linearform der Ordnung L mit $\phi(E) = 0$ und sei $\phi(\sigma E) = a$. *Behauptung*: Es gibt ein σ' in der von σ erzeugten, unter $SL(n, L)$ invarianten Untergruppe G von $GL(n, L)$ und es gibt eine Basis E'_i, $1 \leqq i \leqq n$, mit dualer Basis ϕ'_i, $1 \leqq i \leqq n$, so, dass $\phi'_n(\sigma' E_i) = 0$ für alle i mit $1 \leqq i \leqq n-2$ und so, dass $\phi'_k(\sigma' E'_1) = a$ für ein k mit $1 \leqq k \leqq n-1$.

2.8.3.1. Zum Beweis dieser Behauptung gehen wir aus von einer Basis

E_i, $1 \leqq i \leqq n$, und dualer Basis ϕ_i, $1 \leqq i \leqq n$, so, dass $E = E_1$ und $\phi = \phi_{n-1}$. Die Matrix von σ und die Matrix von σ^{-1} bezüglich dieser Basis sei bezeichnet durch

$$((a_{ik})) = ((\phi_i(\sigma E_k))), \qquad ((b_{ik})) = ((\phi_i(\sigma^{-1} E_k))).$$

Insbesondere ist also $a = \phi_{n-1}(\sigma E_1) = a_{n-1\,1}$.

Wir definieren die Transvektionen τ_j, $j \neq n-1$, durch

$$\tau_j X = X + E_j \phi_{n-1}(X) \qquad (j \neq n-1). \tag{33}$$

Da G invariant ist, gehört auch $\rho_j = \sigma^{-1} \tau_j \sigma \tau_j^{-1}$ zu G. Wir finden

$$\rho_j E_k = E_k + \sigma^{-1} E_j \phi_{n-1}(\sigma E_k) \qquad (j, k \neq n-1). \tag{34}$$

Ferner, für $j \neq n-1$,

$$\rho_j \sigma^{-1} E_j = \sigma^{-1} \tau_j \sigma \tau_j^{-1} \sigma^{-1} E_j = \sigma^{-1} E_j (1 - a_{n-1\,j} b_{n-1\,j}) - E_j b_{n-1\,j}. \tag{35}$$

2.8.3.2. Wir betrachten zunächst den Fall: Es gibt ein r, $2 \leqq r \leqq n$, mit $b_{rn} \in L^*$. In diesem Falle erklären wir eine neue Basis E'_i durch: $E'_i = E_i$ für $i \neq r$ und $E'_r = \sigma^{-1} E_n$.

Für $i < n-1$ und $i \neq r$ haben wir wegen (34)

$$\rho_n E'_i = \rho_n E_i = E_i + \sigma^{-1} E_n \phi_{n-1}(\sigma E_i) = E'_i + E'_r a_{n-1\,i} \tag{36}$$

und für $r \neq n-1$ haben wir wegen (35)

$$\rho_n E'_r = \rho_n \sigma^{-1} E_n = E'_r (1 - a_{n-1\,n} b_{n-1\,n}) - E'_n b_{n-1\,n}. \tag{37}$$

Fall (i) : $r \neq n-1$. Aus (36) und (37) folgt:

$$\phi'_{n-1}(\rho_n E'_i) = 0 \text{ für } i < n-1; \; \phi'_r(\rho_n E'_i) = a_{n-1\,1}$$

Wenn wir also E'_{n-1} und E'_n vertauschen und $\sigma' = \rho_n$ setzen, so folgt, mit $k = r$, die Behauptung 2.8.3.

Fall (ii) : $r = n-1$. Aus (36) und (37) folgt

$$\phi'_n(\rho_n E'_i) = 0 \text{ für } i < n-1; \; \phi'_{n-1}(\rho_n E'_1) = a_{n-1\,1}.$$

Mit $\sigma' = \rho_n$, $k = n-1$ folgt die Behauptung 2.8.3.

2.8.3.3. Wir betrachten den in 2.8.3.2 ausgeschlossenen Fall, dass $b_{rn} \in I$ für alle r, $2 \leqq r \leqq n$. Dann gibt es jedoch ein r, $2 \leqq r \leqq n$, so, dass $b_{r1} \in L^*$, wie man durch Reduktion mod I erkennt. Wir erklären eine neue Basis E'_i durch $E'_i = E_i$ für $i \neq r$, und $E'_r = \sigma^{-1} E_1$. Aus (34) und (35) folgt

$$\rho_1 E'_i = E'_i + E'_r a_{n-1\,i} \text{ für } i \neq n-1,\ i \neq r, \tag{38}$$

$$\rho_1 E'_r = E'_r(1 - a_{n-1\,1} b_{n-1\,1}) - E'_1 b_{n-1\,1}. \tag{39}$$

Fall (i) : $r = n$. Aus (38) und (39) folgt

$$\phi'_{n-1}(\rho_1 E'_i) = 0 \text{ für } i < n-1;\ \phi'_n(\rho_1 E'_1) = a_{n-1\,1}$$

Wenn wir E'_{n-1} und E'_n vertauschen und $\sigma' = \rho_1$ setzen, so folgt, mit $k = r$, die Behauptung 2. 8. 3.

Fall (ii) : $r \neq n$. Aus (38) und (39) folgt

$$\phi'_n(\rho_1 E'_i) = 0 \text{ für } i < n-1;\ \phi'_r(\rho_1 E'_1) = a_{n-1\,1}.$$

Mit $\sigma' = \rho_1$, $k = r$ folgt die Behauptung 2. 8. 3.

2. 8. 4. Wir kommen jetzt zum Beweis der in 2. 8. 2 aufgestellten Behauptung, dass die Gruppe G eine Transvektion der Ordnung (a) enthält. Nach 2. 8. 3 können wir annehmen, dass wir eine Basis E_i, $1 \leqq i \leqq n$, von V haben mit dualer Basis ϕ_i, $1 \leqq i \leqq n$, und ein Element $\sigma \in G$ so, dass

$$\phi_n(\sigma E_i) = 0 \text{ für } i < n-1;\ \phi_k(\sigma E_1) = a \text{ für ein } k,\ 2 \leqq k \leqq n-1. \tag{40}$$

Wir betrachten die Transvektion τ:

$$\tau X = X + E_1 \phi_n(X). \tag{41}$$

Für $\rho = \sigma\tau\sigma^{-1}\tau^{-1} \in G$ finden wir

$$\rho X = X - E_1\phi_n(X) + \sigma E_1 \phi_n(\sigma^{-1}X) - \sigma E_1 \phi_n(\sigma^{-1}E_1)\phi_n(X). \tag{42}$$

Es ist also $\rho X - X \in H$, wo H die von $E_1, \cdots, E_{n-1}$ aufgespannte Hyperbene ist. Daher folgt aus 2. 8. 1, mit $U = E_i$, $1 \leqq i \leqq n-1$: G enthält die Transvektionen mit dem Vektor $\rho E_i - E_i = \sigma E_1 \phi_n(\sigma^{-1}E_i)$, $1 \leqq i \leqq n-1$. Wir unterscheiden zwei Fälle:

2. 8. 4. 1. Eines der Elemente $\phi_n(\sigma^{-1}E_i)$, $1 \leqq i \leqq n-1$, gehört zu L^*. Dann enthält G also eine Transvektion der Ordnung L und mit Satz 2 folgt $SL(n, L) \subset G$, $o(G) = J = L$, es folgt also die Behauptung von Satz 3.

2. 8. 4. 2. Die Elemente $\phi_n(\sigma^{-1}E_i)$, $1 \leqq i \leqq n-1$, gehören alle zu I. Wir bezeichnen mit K das von diesen Elementen erzeugte Ideal. Dann ist also $K \subset I$. K stimmt überein mit dem von den Elementen $\phi_n(\sigma E_i)$, $1 \leqq i \leqq n-1$, erzeugten Ideal; denn $h_K \sigma^{-1} g_K H = g_K H$ impliziert $h_K \sigma g_K H = g_K H$ und umgekehrt. Wegen Satz 2 und dem Schluss von 2. 8. 4 haben wir $SC(n, L, K) \subset G$.

Wir definieren eine Linearform ψ durch

$$\psi(\sigma E_i) = 0 \text{ für } i < n-1; \; \psi(E_n) = 0; \; \psi(\sigma E_{n-1}) = 1. \tag{43}$$

Da die $g_K E_i$, $1 \leqq i \leqq n-1$, durch $h_K \sigma$ unter sich transformiert werden und $K \subset I$, bilden die σE_i, $1 \leqq i \leqq n-1$, zusammen mit E_n, eine Basis für V; daher ist ψ durch (43) wohldefiniert.

Wir betrachten die Transvektion μ:

$$\mu X = X + E_n \phi_n(\sigma E_{n-1}) \psi(X). \tag{44}$$

Offenbar ist $o(\mu) \subset K$, also $\mu \in G$. Dann gilt auch $\sigma' = \mu^{-1}\sigma \in G$. Wir finden

$$\sigma' E_i = E_i, \; i < n-1; \; \sigma' E_{n-1} = \sigma E_{n-1} - E_n \phi_n(\sigma E_{n-1}).$$

Es ist also $\sigma' H = H$, wo $H = \phi_n^{-1}(0)$. Folglich $\phi_n \sigma'^{-1} = d\phi_n$, mit $d \in L^*$.

Mit der Tranvektion τ, (41), erhalten wir für $\rho' = \sigma' \tau \sigma'^{-1} \tau^{-1} \in G$ nach (42) den Ausdruck

$$\rho' X = X + (\sigma E_1 d - E_1) \phi_n(X). \tag{45}$$

ρ', (45), ist also eine Transvektion der Ordnung $o(\sigma E_1 d - E_1) \supset (\phi_K(\sigma E_1)) = (a)$. Nach Satz 2 enthält G also eine Transvektion der Ordnung (a). Damit ist die Behauptung in 2.8.2 bewiesen, und also Satz 3 bewiesen.

2.9. Das Theorem 3 ist eine Zusammenfassung der vorstehend bewiesenen Ergebnisse.

UNIVERSITÄT GÖTTINGEN, GERMANY.

LITERATURVERZEICHNIS.

[1] E. Artin, *Geometric Algebra*, New York, 1957.

[2] J. Brenner, "The linear homogeneous group," *Annals of Mathematics*, vol. 39 (1938), pp. 472-493. "The linear homogeneous group, II," *ibid.*, vol. 45 (1944), pp. 100-109.

[3] H. Cartan-S. Eilenberg, *Homological Algebra*, Princeton, 1956.

[4] J. Dieudonné, *Sur les groupes classiques*, Paris, 1948.

[5] ———, *La géométrie des groupes classiques*, Berlin, 1955.

[6] W. Klingenberg, "Linear groups over local rings," *Bulletin of the American Mathematical Society*, vol. 66 (1960), pp. 294-296.

[7] ———, "Lineare Gruppen über verallgemeinerten Bewertungsringen," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* (to appear).

ON DIFFERENTIAL EQUATIONS AND THE FUNCTION $J_\mu^2+Y_\mu^2$.*[1]

By PHILIP HARTMAN.

Introduction. Let $J_\mu = J_\mu(t)$, $Y_\mu = Y_\mu(t)$ denote Bessel functions of a non-negative order μ of the first and second kind, respectively, and let t be real. It is known that $t(J_\mu^2+Y_\mu^2)$ is increasing or decreasing for $t>0$ according as $\mu<\frac{1}{2}$ or $\mu>\frac{1}{2}$ and that $(t^2-\mu^2)^{\frac{1}{2}}(J_\mu^2+Y_\mu^2)$ is increasing for $t \geqq \mu \geqq 0$; cf. [9], p. 446. These facts are usually derived from Nicholson's integral formula for $J_\mu^2+Y_\mu^2$, the proof of which is rather involved. It seems, therefore, of interest to obtain these assertions directly from simple, general theorems on differential equations.

Let $q=q(t)$ be a continuous, positive function for large t. General conditions (cf. [11]) are known which imply that

$$u''+q(t)u=0 \tag{0.1}$$

has a pair of real-valued solutions $u=x(t), y(t)$ satisfying, as $t\to\infty$, asymptotic formulae similar to

$$\begin{aligned} q^{\frac14}z &= \exp i\int^t q^{\frac12}(s)ds+o(1), \\ (q^{\frac14}z)' &= iq^{\frac34}\exp i\int^t q^{\frac12}(s)ds+o(1), \end{aligned} \tag{0.2}$$

where $z=x+iy$. But these results give no information on the possible monotone character of $q^{\frac14}|z|$ or on sharp bounds for $q^{\frac14}|z|$ for all t-values under consideration. The object of Part I of this paper is to supply such information. It will be shown there that, under suitable conditions on q, the number 1 is a bound for $q|z|^4$ and that this implies the monotony of $|z|$. The question of the monotony of $q|z|^4$ can be decided in many cases by examining the applicability of this result to the differential equation having $q^{\frac14}x$, $q^{\frac14}y$ as solutions; cf. the change of variables (2.7) below.

These results will be applied in Section 4 to the Bessel functions. It

---

* Received November 15, 1960.

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under contract No. AF 18(603)-41. Reproduction in whole or in part is permitted for any purpose of the United States Government.

will be seen that they imply, in particular, that $z = t^{\frac{1}{2}}(J_\mu + iY_\mu)$ satisfies, for $t > 0$,

$$(0.3) \qquad |z| > 0, \qquad |z|' \leqq 0, \qquad |z|'' \geqq 0$$

or

$$(0.4) \qquad |z| > 0, \qquad |z|' \geqq 0, \qquad |z|'' \leqq 0$$

according as $\mu > \frac{1}{2}$ or $\mu \leqq \frac{1}{2}$. Note that the last part of (0.3), $|z|'' \geqq 0$, is not implied by the following consequence

$$(0.5) \qquad |z|^2 > 0, \ (|z|^2)' \leqq 0, \ (|z|^2)'' \leqq 0, \ (|z|^2)''' \geqq 0, \cdots$$

of Nicholson's formula (for $\mu \geqq \frac{1}{2}$).

On the other hand, the results and methods of Part I do not lead to the sequence of inequalities in (0.5). The question of higher order monotony of $|z(t)|^2$, where $z = x(t) + iy(t)$ is a complex-valued solution of a general equation (0.1), will be examined in Part IV. The results to be obtained will depend on Parts II and III which deal with differential equations of arbitrary order. The methods to be employed will be very different from and do not depend on those in Part I.

It will remain undecided whether or not the results on the higher order monotony of $|z|^2$ can be sharpened to give such results about $|z|$.

Applications of the results of Part IV to Bessel functions give the complete monotony (i.e., (0.5)) for $|z|^2 = t(J_\mu^2 + Y_\mu^2)$ for $t > 0$ when $\mu > \frac{1}{2}$. This proof is longer than the one involving Nicholson's formula but has the advantage of applying to a large class of differential equations.

It can be mentioned that Nicholson's formula implies that, when $\mu < \frac{1}{2}$, the derivative of $|z|^2 = t(J_\mu^2 + Y_\mu^2)$ is completely monotone for $t > 0$. It will remain undecided how to derive this result from a general theory of differential equations. A partial result in this direction is given in Section 22.

Part I. Monotony and convexity of $|z|$.

This part of the paper concerns inequalities of the form (0.3) or (0.4) for some complex-valued solution $u = z(t)$ of (0.1). The main result is Theorem 3.1.

1. Bounds for solutions. Let $Q = Q(s)$ be a continuous, monotone function of s for $s > S$ satisfying, as $s \to \infty$,

$$(1.1) \qquad Q \to 1.$$

Then

$$d^2U/ds^2 + Q(s)U = 0 \tag{1.2}$$

has a pair of real-valued solutions $U = X(s), Y(s)$ such that $Z = X + iY$ satisfies, as $s \rightarrow \infty$,

$$Z = \exp i \int^s Q^{\frac{1}{2}}(\tau)\,d\tau + o(1), \qquad Z_s = iZ + o(1), \tag{1.3}$$

where $Z_s = dZ/ds$; [12], Appendix. The solution $U = Z(s)$ of (1.2) satisfying (1.3) is uniquely determined, up to constant factors, by the requirement that

$$Z_s/Z \rightarrow i \quad \text{as} \quad s \rightarrow \infty; \tag{1.4}$$

[6]. In view of (1.3), the (constant) Wronskian of X and Y has the value 1,

$$XY_s - X_sY = 1. \tag{1.5}$$

LEMMA 1.1. *Let $Q = Q(s)$ be positive, continuous and monotone for $S < s < \infty$ and satisfy* (1.1). *Let $U = Z(s)$ be the solution of* (1.2) *satisfying* (1.3) *as $s \rightarrow \infty$. Then, for $s > S$,*

$$|Z|^2Q \leqq 1 \leqq |Z|^2 \text{ and } |Z_s|^2 \leqq 1 \leqq |Z_s|^2/Q \tag{1.6$_1$}$$

or

$$|Z|^2Q \geqq 1 \geqq |Z|^2 \text{ and } |Z_s|^2 \geqq 1 \geqq |Z_s|^2/Q \tag{1.6$_2$}$$

according as

(1.7$_1$) $dQ \geqq 0$ *or* (1.7$_2$) $dQ \leqq 0$.

It will be clear from the proof that the interval $S < s < \infty$ can be replaced by an interval $S < s < S^*(\leqq \infty)$, if the assumptions (1.1), (1.3) refer to $s \rightarrow S^*$. If $S^* < \infty$, then Q can be defined at $s = S^*$ by $Q(S^*) = 1$ and is then continuous for $S < s \leqq S^*$. The existence of a solution $U = Z(s)$ satisfying (1.3) is obvious.

Remark 1. In addition to (1.6), it can be shown that

$$|Z|^2Q + |Z_s|^2 \leqq 1 + Q \tag{1.8}$$

holds in both cases (1.7$_1$) and (1.7$_2$). It will be clear that strict inequality holds in (1.6) and (1.8) if $Q(s) \not\equiv 1$ for large s.

Remark 2. The inequality $|Z|^2 \geqq 1$ in (1.6$_1$) holds for $s > S$ if the conditions $Q > 0$, $dQ \geqq 0$ for $s > S$ are replaced by $Q(s) \leqq 0$ for $S < s \leqq S_0$

and $Q(s) > 0$, $dQ(s) \geqq 0$ for $s > S_0$, where S_0 is some fixed number. Note that Q is not required to be monotone on the interval $S < s \leqq S_0$.

Proof of Lemma 1.1. If (1.2) is divided by $Q(s)$ and differentiated with respect to s, and the result divided by $Q(s)$, one obtains the equation

$$d^2W/d\tau + Q^{-1}(s)W = 0, \text{ where } s = s(\tau),$$

and

$$W = U', \; d\tau = Q(s)\,ds, \text{ and } dW/d\tau = U''/Q = -U.$$

This makes it clear that it is sufficient to consider only the case (1.6_1)-(1.7_1). (This change of variables, which will be used several times in this paper, is suggested in part by Wintner [13]; cf. [3].)

Let $U = U(s)$ be any real-valued solution of (1.2). Then, by virtue of (1.2) and (1.7_1),

$$(1.9) \quad d(U^2Q + U_s^2) = U^2dQ \geqq 0 \text{ and } d(U^2 + U_s^2/Q) = -(U_s/Q)^2dQ \leqq 0.$$

For arbitrarily fixed real ϕ, let

$$(1.10) \qquad U = X(s)\cos\phi + Y(s)\sin\phi;$$

so that (1.1) and (1.3) imply $U^2Q + U_s^2 \rightarrow 1$ and $U^2 + U_s^2/Q \rightarrow 1$ as $s \rightarrow \infty$. Hence, by (1.9), for $s > S$,

$$(1.11) \qquad U^2Q + U_s^2 \leqq 1 \text{ and } U^2 + U_s^2/Q \geqq 1.$$

The first inequality in (1.11) shows that $U^2Q \leqq 1$ for $s > S$ and for every ϕ. For a fixed s, choose ϕ in (1.10) so that $U(s) = (X^2(s) + Y^2(s))^{\frac{1}{2}} = |Z|$. Then, for this value of s, it is seen that $|Z|^2Q = U^2Q \leqq 1$.

The second inequality in (1.11) implies that $U^2(s) \geqq 1$ if $U_s(s) = 0$. For a fixed s, choose ϕ so that $U_s(s) = 0$. By Cauchy's inequality, $U^2(s) \leqq |Z(s)|^2$. Thus, for this value of s, $|Z(s)|^2 \geqq U^2(s) \geqq 1$.

This proves the first two inequalities in (1.6_1). The last two are proved similarly. Hence Lemma 1.1 follows.

On Remark 1. Again, only the case (1.6_1)-(1.7_1) will be considered. In view of (1.10), the expression $U^2Q + U_s^2$ is a quadratic form in $(\cos\phi, \sin\phi)$ for a fixed s. According to (1.11), the eigenvalues λ of this form satisfy $\lambda \leqq 1$. It is readily verified, if use is made of (1.5), that the eigenvalues λ of this form are the roots of the equation $\lambda^2 - \lambda(|Z|^2Q + |Z_s|^2) + Q = 0$. The inequality (1.8) merely expresses the fact that the largest root of this equation is at most 1.

On Remark 2. In view of Lemma 1.1, it follows that $|Z(s)| \geqq 1$, $|Z_s(s)| \leqq 1$ for $s \geqq S_0$. Choose ϕ so that $\cos\phi = Y_s(S_0)/|Z_s(S\ )|$, $\sin\phi = -X_s(S_0)/|Z_s(S_0)|$. Then $U(s)$ in (1.10) satisfies

$$U(S_0) = (XY_s - X_sY)/|Z_s| = 1/|Z_s(S_0)| \geqq 1, \quad U_s(S_0) = 0.$$

Initial conditions $U(S_0) > 0$, $U_s(S_0) = 0$ at $s = S_0$ and $Q \leqq 0$ for $S < s \leqq S_0$ imply, by a simple convexity argument, that $dU(s) \leqq 0$ on this interval. Hence $U(s) \geqq U(S_0) = 1$ for $S < s \leqq S_0$. Cauchy's inequality gives therefore $|Z(s)| \geqq U(s) \geqq 1$.

2. Bounds for $q\,|z|^4$.

The desired inequalities for solutions of (0.1) do not follow directly from Lemma 1.1 but can be obtained from this lemma after a standard change of variables (Riemann-Liouville).

LEMMA 2.1. *Let* $q(t)$ *be a positive function of class* C^2 *for* $t > T_0$ *with the properties that*

$$Q \equiv 1 + 5q'/16q^3 - q''/4q^2 \equiv 1 - (q'/q^{\frac{5}{4}})'/4q^{\frac{3}{4}} \tag{2.1}$$

satisfies $Q(t) \to 1$ *as* $t \to \infty$ *and that either*

$$dQ \leqq 0 \text{ for } t > T_0 \tag{2.2$_1$}$$

or there exists a $T_1 \geqq T_0$ *such that*

$$Q \leqq 0 \text{ for } T_0 < t \leqq T_1 \text{ and } Q > 0,\ dQ \geqq 0 \text{ for } t > T_1. \tag{2.2$_2$}$$

Then (0.1) *possesses a pair of real-valued solutions* $u = x(t), y(t)$ *such that* $z = x + iy$ *satisfies, as* $t \to \infty$,

$$q^{\frac{1}{4}}z \sim \exp i \int^t Q^{\frac{1}{2}}(\tau)\, q^{\frac{1}{2}}(\tau)\, d\tau, \qquad (q^{\frac{1}{4}}z)' \sim iq^{\frac{1}{2}}(q^{\frac{1}{4}}z); \tag{2.3}$$

$$xy' - x'y = 1; \tag{2.4}$$

and, for $t > T_0$, *either*

(2.5$_1$) $\quad q\,|z|^4 \leqq 1 \quad$ *or* $\quad$ (2.5$_2$) $\quad q\,|z|^4 \geqq 1$

according as (2.2$_1$) *or* (2.2$_2$) *holds.*

If q is of class C^3, then $Q(t)$ has a derivative given by

$$Q' = (18qq'q'' - 15q'^3 - 4q^2q''')/16q^4.$$

Note that $dQ \geqq 0$ is implied by

$$q > 0,\ q' \geqq 0,\ q'' \leqq 0,\ q''' \geqq 0. \tag{2.6}$$

Proof. By the Riemann-Liouville change of variables,

$$U = uq^{\frac{1}{4}} \quad \text{and} \quad ds = q^{\frac{1}{2}}(t)\,dt, \tag{2.7}$$

the differential equation (0.1) is transformed into (1.2), where Q is defined by (2.1) and $t = t(s)$. The interval $T_0 < t < \infty$ is changed into some interval $(-\infty \leqq)\, S < s < S^{\infty} \leqq \infty$.

By Lemma 1.1 and the Remark 2, (1.2) has a pair of real-valued solutions $U = X, Y$ satisfying (1.3), as $s \rightarrow S^*$, and $|Z| \leqq 1$ for $s > S$ according as (2.2_1) or (2.2_2) holds. If

$$x = X/q^{\frac{1}{4}}, \qquad y = Y/q^{\frac{1}{4}} \tag{2.8}$$

(cf. (2.7)) are the corresponding solutions of (0.1), then (2.3) and the assertion concerning (2.5) follow.

3. Monotony and convexity of $|z|$. The main theorem of this part of the paper can be obtained as a consequence of Lemma 2.1.

THEOREM 3.1. *Let $q(t)$ satisfy the conditions and $x(t), y(t)$ the assertions of Lemma* 2.1.

(i) *Let $Q(t)$ be in case (2.2_1). Then*

$$|z| > 0, \qquad |z|'' \geqq 0 \tag{3.1}$$

for $t > T_0$. If, in addition, $q(t)$ is continuous for $t > 0$ and $q(t) \leqq 0$ for $0 < t \leqq T_0$, then (3.1) *holds for $t > 0$. If $z(t)$ remains bounded as $t \rightarrow \infty$ (that is, if $q(t) \geqq \text{const.} > 0$ for large t), then, for $t > 0$,*

$$|z| > 0, \qquad |z|' \leqq 0, \qquad |z|'' \geqq 0. \tag{3.2}$$

(ii) *Let $Q(t)$ be in case (2.2_2). Then, for $t > T_0$,*

$$|z| > 0, \qquad |z|' \geqq 0, \qquad |z|'' \leqq 0. \tag{3.3}$$

It is readily verified from the last part of (2.1) that if q and Q are monotone and $0 < q(\infty) \leqq \infty$, then $Q \rightarrow 1$ as $t \rightarrow \infty$. This gives the following

COROLLARY. *If $q(t) \leqq 0$ for $0 < t \leqq T_0$ and* (2.6) *holds for $t > T_0$, then* (3.2) *holds for $t > 0$.*

Strict inequality holds in the inequalities in (3.1), (3.2), (3.3) unless $Q \equiv 1$ for large t, that is, unless $q(t) \equiv (c_1 t + c_2)^{-4}$ for large t, where c_1, c_2 are constants.

If the half-line $t > T_0$ is replaced by a finite interval, then the inequalities $|z|' \leqq 0$ in (3.2) and $|z|' \geqq 0$ in (3.3) need not be valid.

Proof of Theorem 3.1. If $u = x(t), y(t)$ are solutions of (0.1) satisfying (2.4), then two differentiations of $r = |z| = (x^2 + y^2)^{\frac{1}{2}}$ show that

$$(3.4) \qquad r'' = -qr + r^{-3} = r^{-3}(1 - qr^4).$$

In case (2.2_1), the relation (2.5_1) holds for $t > T_0$. It also holds for $t > T$ if $q \leqq 0$ for $T < t \leqq T_0$. Hence $r'' \geqq 0$ for all t under consideration. This gives (3.1) and, hence, (3.2) if $r(t)$ is bounded as $t \rightarrow \infty$.

In the case (2.2_2), the relation (2.5_2) holds and implies $r'' \leqq 0$ for $t > T_0$. Since $r > 0$, this gives (3.3).

4. Applications to Bessel functions. The functions $v = J_\mu(t)$, $Y_\mu(t)$ are real-valued linearly independent solutions of the Bessel equation

$$(4.1) \qquad v'' + v'/t + (1 - \mu^2/t^2)v = 0.$$

Hence $u = t^{\frac{1}{2}}J_\mu(t)$, $t^{\frac{1}{2}}Y_\mu(t)$ are real-valued solutions of

$$(4.2) \qquad u'' + (1 - \alpha/t^2)u = 0, \text{ where } \alpha = \mu^2 - \tfrac{1}{4}.$$

Note that

$$(4.3) \qquad \alpha >, =, < 0 \text{ according as } (0 \leqq)\ \mu >, =, < \tfrac{1}{2}.$$

Furthermore,

$$(4.4) \qquad z = x(t) + iy(t) = (\tfrac{1}{2}\pi t)^{\frac{1}{2}} e^{i\theta}(J_\mu(t) - iY_\mu(t)),$$

where $\theta = \frac{1}{2}(\mu + \frac{1}{2})\pi$, is a solution of (4.2) satisfying

$$(4.5) \qquad z = e^{it} + o(1),\ z' = ie^{it} + o(1) \text{ as } t \rightarrow \infty.$$

If (4.2) is identified with (1.2), Lemma 1.1 and the Remark 2 following it give the inequalities

$$(4.6) \qquad t(J_\mu^2 + Y_\mu^2)(1 - \alpha/t^2) < 2/\pi < t(J_\mu^2 + Y_\mu^2) \text{ if } \mu > \tfrac{1}{2},$$

$$(4.7) \qquad t(J_\mu^2 + Y_\mu^2)(1 - \alpha/t^2) > 2/\pi > t(J_\mu^2 + Y_\mu^2) \text{ if } \mu < \tfrac{1}{2},$$

for $t > 0$. Inequalities of this type were obtained by Schafheitlin [7], p. 86.

If (4.2) is identified with (0,1), so that $q = 1 - \alpha/t^2$, then the corresponding function (2.1) is

$$(4.8) \qquad Q = 1 + 5\alpha^2/4(t^2 - \alpha)^3 + 3\alpha/2(t^2 - \alpha)^2$$

for $t^2 > \max(0, \alpha)$. If $\mu > \frac{1}{2}$ (i. e., $\alpha > 0$), then Q satisfies (2.2_1) with $T_0 = \alpha^{\frac{1}{2}}$, so that (2.4_1) is valid and becomes

$$(4.9) \qquad (t^2 - \mu^2 + \tfrac{1}{4})^{\frac{1}{2}}(J_\mu{}^2 + Y_\mu{}^2) < 2/\pi \text{ if } t > (\mu^2 - \tfrac{1}{4})^{\frac{1}{2}} \text{ and } \mu > \tfrac{1}{2}.$$

If $\mu < \frac{1}{2}$ (i. e., $\alpha < 0$), then Q satisfies (2.2_2) with $T = 0$, $T_1 = \frac{1}{2}(-\alpha)^{\frac{1}{2}}$ and (2.4_2) gives

$$(4.10) \qquad (t^2 - \mu^2 + \tfrac{1}{4})^{\frac{1}{2}}(J_\mu{}^2 + Y_\mu{}^2) > 2/\pi \text{ if } t > 0 \text{ and } \mu < \tfrac{1}{2}.$$

It also follows from Theorem 3.1 that $r = t^{\frac{1}{2}}(J_\mu{}^2(t) + Y_\mu{}^2(t))^{\frac{1}{2}}$ satisfies $r > 0$, $r' < 0$, $r'' > 0$ or $r > 0$, $r' > 0$, $r'' < 0$ for $t > 0$ according as $\mu > \frac{1}{2}$ or $0 \leqq \mu < \frac{1}{2}$.

The inequality (4.10) contrasts sharply with the known inequality

$$(4.11) \qquad (t^2 - \mu^2)^{\frac{1}{2}}(J_\mu{}^2 + Y_\mu{}^2) < 2/\pi \text{ if } t \geqq \mu \geqq 0$$

usually deduced from Nicholson's formulae, cf. [9], p. 447. If $\mu \geqq \frac{1}{2}$, the last inequality is contained in (4.9); a derivation of (4.11) based on the results of Sections 1-3 will be indicated.

If $t = e^s$, then the Bessel equation (4.1) becomes

$$(4.12) \qquad v_{ss} + (t^2 - \mu^2)v = 0, \text{ where } t = e^s.$$

The change of variables analogous to (2.7),

$$(4.13) \qquad V = (t^2 - \mu^2)^{\frac{1}{4}}v, \qquad d\sigma = (t^2 - \mu^2)^{\frac{1}{2}}ds, \text{ where } t > \mu,$$

transforms (4.12) into an equation

$$(4.14) \qquad V_{\sigma\sigma} + RV = 0,$$

where

$$R = 1 + (e^{4s} + 4\mu^2 e^{2s})/(e^{2s} - \mu^2)^3 \text{ and } s = s(\sigma).$$

The equation has the pair of solutions $V = (t^2 - \mu^2)^{\frac{1}{4}}J_\mu$, $(t^2 - \mu^2)^{\frac{1}{4}}Y_\mu$, where $t = e^s > \mu$ and $s = s(\sigma)$. In terms of s, the coefficient R can be written as

$$(4.15) \qquad R = 1 + (e^{-2s}/4 + \mu^2 e^{-4s})\,(\sum_{k=0}^{\infty} \mu^{2k} e^{-2ks})^3, \quad e^s > \mu.$$

It is clear that R is a decreasing function of s (hence σ), so that (1.6_2) in Lemma 1.1 applied to (4.14) gives (4.11).

It can also be verified from Theorem 3.1 applied to (4.14) that $r = (t^2 - \mu^2)^{\frac{1}{2}}(J_\mu{}^2 + Y_\mu{}^2)$ is increasing for $t \geqq \mu \geqq 0$; cf. [9], pp. 446-447.

The inequalities (4.9), (4.10), (4.11) suggest the examination of the function $(t^2-\mu^2+\beta)^{\frac{1}{2}}(J_\mu^2+Y_\mu^2)$, where $\beta \geqq 0$ is a constant. Note that if the Riemann-Liouville change of variables (2.7) is altered to

$$(4.16)\qquad U=(q+\beta)^{\frac{1}{4}}u, \qquad ds=(q+\beta)^{\frac{1}{2}}dt,$$

then (0.1) is transformed into

$$(4.17)\qquad U_{ss}+[1+5q'^2/16(q+\beta)^3-q''/4(q+\beta)^2-\beta/(q+\beta)]U=0.$$

Correspondingly, if (4.13) is replaced by

$$(4.18)\qquad V=(t^2-\gamma)^{\frac{1}{4}}v, \qquad d\sigma=(t^2-\gamma)^{\frac{1}{2}}ds, \text{ where } t^2=e^{2s}>\gamma$$

and $\gamma=\mu^2-\beta$, then (4.12) is transformed into (4.14), where

$$(4.19)\qquad R=1+[e^{4s}(1-4\beta)+4\gamma e^{2s}(1+2\beta)-4\beta\gamma^2]/4(e^{2s}-\gamma)^3.$$

From the relation

$$(4.20)\qquad R_s=-[(1-4\beta)e^{6s}+2\gamma(5+4\beta)e^{4s}$$
$$+4\gamma^2(1-\beta)e^{2s}]/2(e^{2s}-\gamma)^4,$$

it is clear that there exists a $T=T(\beta,\mu)>0$ such that according as $\beta>\frac{1}{4}$ or $\beta<\frac{1}{4}$, R is increasing or decreasing for $t \geqq T$. Thus, by Lemma 1.1, for $\mu \geqq 0$,

$$(4.21)\qquad (t^2-\mu^2+\beta)^{\frac{1}{2}}(J_\mu^2+Y_\mu^2)>2/\pi \text{ if } t>T \text{ and } \beta>\tfrac{1}{4},$$

$$(4.22)\qquad (t^2-\mu^2+\beta)^{\frac{1}{2}}(J_\mu^2+Y_\mu^2)<2/\pi \text{ if } t>T \text{ and } \beta>\tfrac{1}{4}.$$

These inequalities reduce to (4.9), (4.10) if $\beta=\frac{1}{4}$.

Obviously, T can be chosen to be 0 [or $\gamma^{\frac{1}{2}}=(\mu^2-\beta)^{\frac{1}{2}}$] in (4.21) [or (4.22)] if $\beta \geqq 1$ and $\mu \leqq \beta^{\frac{1}{2}}$ (so that $\gamma \leqq 0$) [or $\beta \leqq \frac{1}{4}$ and $\mu \geqq \beta^{\frac{1}{2}}$ (so that $\gamma \geqq 0$)].

Part II. An inhomogeneous second order equation.

5. Preliminaries. The familiar "alternating series argument" shows that if $f(t)$ is continuous for $t>0$, $f(t) \geqq 0$, $df(t) \leqq 0$ and $f(t) \rightarrow 0$ as $t \rightarrow \infty$, then

$$(5.1)\qquad w(t)=\int_t^\infty f(s)\sin(s-t)\,ds$$

is convergent and non-negative for $t>0$. In addition, if $f(t)$ is convex, then

$$(5.2)\qquad w'(t)=-\int_t^\infty f(s)\cos(s-t)\,ds$$

is non-positive. Furthermore, the two implications $f \geqq 0$, $f' \leqq 0 \Rightarrow w \geqq 0$ and $f \geqq 0$, $f' \leqq 0$, $f'' \geqq 0 \Rightarrow w' \geqq 0$, $w' \leqq 0$ are the first two of an infinite sequence of implications. This is clear if it is noted that (5.1) is the unique solution of

$$w'' + w = f(t) \tag{5.3}$$

satisfying $w \rightarrow 0$ as $t \rightarrow \infty$.

It will be shown below that similar facts are valid for a particular solution of the more general second order equation

$$w'' + q(t)w = f(t) \tag{5.4}$$

under suitable qualitative conditions on q. (The results will be extended to linear and non-linear differential equations of higher order in Part III.)

Consider the homogeneous equation belonging to (5.4),

$$v'' + q(s)v = 0. \tag{5.5}$$

It will be assumed below that (5.5) is oscillatory at $s = \infty$, i.e., that every solution $v = v(s)$ of (5.5) has infinitely many zeros custerilng at $s = \infty$.

A Green's function $G(t, s)$ for $s \geqq t$ for (5.5) will be needed. This will be defined as follows: Let t be fixed. For $s \geqq t$, let $v(s) = G(t, s)$ be the solution of (5.5) determined by the initial condition,

$$G(t, s) = 0 \text{ and } G_s(t, s) = 1 \text{ if } s = t. \tag{5.6}$$

The analogues of (5.3) and (5.1) are (5.4) and

$$w(t) = \int_t^\infty G(t, s) f(s)\, ds. \tag{5.7}$$

Formally, the derivative of (5.7) is

$$w'(t) = \int_t^\infty G_t(t, s) f(s)\, ds, \tag{5.9}$$

since $G(s, s) = 0$.

The results of Part II deal with the "order of monotony" of the particular solution (5.7) of (5.4).

Many of the arguments will depend on the fact that if $v = v(s)$ is a solution of (5.5) and q is positive and monotone, then (5.5) implies that

$$d(v^2 + v'^2/q) = v'^2 d(1/q), \tag{5.10}$$

$$d(qv^2 + v'^2) = v^2 dq. \tag{5.11}$$

Hence, $v^2 + v'^2$ and $qv^2 + v'^2$ are monotone. In particular, the sequence of maxima of $|v|$ and $|v'|$ are monotone (since these maxima occur when $v' = 0$ and $v = 0$, respectively).

6. Order of monotony of (5.7). In order to state the results succinctly, it will be convenient to introduce the following terminology:

Definition 6.1. A function $f(t)$ will be said to be of class $M_n(a, b)$ or monotone of order n on $a < t < b$ if it has n ($\geqq 0$) continuous derivatives $f, f', \cdots, f^{(n)}$ satisfying

$$(6.1_j) \qquad (-1)^j f^{(j)}(t) \geqq 0$$

for $j = 0, \cdots, n$ and $a < t < b$. M_n will be an abbreviation for $M_n(0, \infty)$.

In all of the theorems below where it is assumed that $n > 0$ and that certain functions $f, q', q_j, \cdots$ are of class $M_n(a, b)$, the assumption of the existence and continuity of the n-th derivative and the inequality corresponding to (6.1_n) can be weakened to the assumption that the $(n-1)$-st derivative multiplied by $(-1)^{n-1}$ is non-increasing. In fact, if $n > 1$, the conditions on the $(n-1)$-st and n-th derivatives can be replaced by the conditions that the $(n-2)$-nd derivative multiplied by $(-1)^{n-2}$ is non-decreasing and is convex.

Definition 6.2. $f(t)$ will be said to be of class $M_{nm}(T_0, \infty)$ if $f \in M_n(T, \infty)$ and f has m derivatives for $t > T_0$ satisfying

$$(6.2_j) \qquad f^{(j)}(t) \rightarrow 0 \text{ as } t \rightarrow \infty$$

for $j = 0, \cdots, m$. (Note that $f \in M_{n0}(T_0, \infty)$ implies that $f \in M_{n,n-1}(T_0, \infty)$ if $n \geqq 1$. Thus the essential cases of $M_{nm}(T_0, \infty)$ are $m = 0$ and $m \geqq n$.) In analogy with the above, $M_{nm} \equiv M_{nm}(0, \infty)$.

THEOREM 6.1$_n$. *Let $n \geqq 0$. Let $q(t)$ have a derivative $q'(t)$ of class M_n and let $0 < q(\infty) \leqq \infty$. Let $f(t)$ be of class $M_{n+1,0}$. Then* (5.4) *has a unique solution* (*given by* (5.7)) *of class $M_{n,n+2}$.*

Remark 1. Under the assumptions on q, the only solution $v = v(s)$ of the homogeneous equation (5.5) satisfying $v'(s) \rightarrow 0$ as $s \rightarrow \infty$ is $v \equiv 0$. (In fact, by (5.11), the successive maxima of $|v'(s)|$ are non-decreasing.) Hence, (5.4) has at most one solution satisfying $w' \rightarrow 0$ as $t \rightarrow \infty$. Also, if $0 < q(\infty) < \infty$, then (5.4) has at most one solution satisfying $w \rightarrow 0$ as $t \rightarrow \infty$.

Remark 2. If all solutions of (5.5) tend to 0 as $t \rightarrow \infty$ (e. g., if "$q(t) \rightarrow \infty$

smoothly as $t \to \infty$," cf. [2]), then the condition $f(\infty) = 0$ implicit in $f \in M_{n+1,0}$ can be omitted in Theorem 6.1_n except for assertion $w'' \to 0$ when $n = 0$.

Remark 3. Suppose that there is a $t = T_0$, $0 \leqq T_0 < \infty$, such that $q \leqq 0$ or $q > 0$ according as $0 < t \leqq T_0$ or $t > T_0$. For $n > 0$ and $0 < t < T_0$, the conditions on q and f can then be lightened somewhat: for $n = 1$ and $n = 2$, it is sufficient to require only $q \leqq 0$, $f \geqq 0$; for $n > 2$, it is sufficient to require that $q', f \in M_{n-2}(0, T_0)$. If the assertion $w \in M_{n,n+2}$ is weakened to $w \in M_{n,2}$ for $n = 1, 2$, the conditions can also be lightened for $t > T_0$: for $n = 1$, it is sufficient to require that q is non-decreasing, $f \geqq 0$ is non-increasing with $f(\infty) = 0$ and f/q is convex; for $n = 2$, it is sufficient to impose the additional condition that $-(f/q)'$ is convex.

Remark 4. The proof of Theorem (6.1_0) will give the following a priori bounds for w and w':

$$(6.3) \qquad 0 \leqq w(t) \leqq \pi f(t)/q(t), \qquad |w'(t)| \leqq \pi f(t)/q^{\frac{1}{2}}(t);$$

cf. (7.6) below. The upper bound for w is improved successively to $2f(t)/q(t)$ and $f(t)/q(t)$ in the proofs of Theorems 6.1_1 and 6.1_2; cf. (8.4) and (9.2).

Theorem 6.1_n and the theorem of Hausdorff-Bernstein imply the following:

COROLLARY. *Let q, f satisfy the conditions of Theorem 6.1_n for $n = 1, 2, \cdots$, then the solution* (5.7) *of* (5.4) *has a representation as a Laplace-Stieltjes integral*

$$(6.4) \qquad w(t) = \int_0^\infty e^{-st} d\sigma(s) \text{ for } t > 0$$

with some non-decreasing weight function $\sigma = \sigma(s)$.

Theorems 6.1_0, 6.1_1, 6.1_2 and the corresponding Remark 3 will be proved in Sections 7, 8, 9 below. Theorem 6.1_n with $n > 2$ is more subtle and does not seem to follow from the cases $n \leqq 2$ by successive differentiation. In fact, its proof will involve a new existence proof for each n for a differential equation of order $n - 2$. Theorem 6.1_n, with $n > 2$, will be proved in Sections 16-17 in Part III below.

Theorem 6.1_n deals with the case of a non-decreasing q. In order to state analogous theorems for the case of a non-decreasing q, it will be convenient to introduce the following definition:

Definition 6.3. Let the classes of functions $DM_n(a, b)$, DM_n, $DM_{nm}(T_0, \infty)$, DM_{nm} be defined as the analogues of $M_n(a, b)$, M_n, $M_{nm}(T_0, \infty)$,

M_{nm} in which the j-th derivative $f^{(j)} = d^jf/dt^j$ on (6.1_j) and/or (6.2_j) is replaced by $D^{(j)}f$, where D is the differential operator $q^{-1}(t)d/dt$.

THEOREM 6.2_n. *Let* $n \geqq 0$. *Let* $q(t)$ *be continuous, non-increasing and let* (5.5) *be oscillatory at* ∞ *(in particular,* $q > 0$*). Let* $1/q^2$ *have a derivative of class* DM_n. *Let* f/q *be of class* $DM_{n+1,0}$. *Then* (5.4) *has a unique solution* $w = w(t)$ *(given by* (5.7)*) of class* $M_{0,2}$ *and, if* $n > 0$, *then* $-w'$ *is of class* $DM_{n-1,n+1}$.

Theorem 6.2_0 will be proved in Section 10. Theorem 6.2_n, with $n > 0$, will be deduced from Theorem 6.1_{n-1} in Section 11.

7. Proof of Theorem 6. $\mathbf{1_0}$. Note that $q(s) \geqq q(t) > 0$ for $s \geqq t > T_0$. Thus, if $v = v(s) \not\equiv 0$ is a solution of (5.5), then the graph of $y = |v(s)|$ consists of a sequence of "arches." The first and second comparison theorems of Sturm imply that if the k-th arch is over the interval $s_k \leqq s \leqq s_{k+1}$ and $q(s_0) \leqq q(s^0)$ when $s_{k-1} \leqq s_0 \leqq s_k \leqq s^0 \leqq s_{k+1}$, then a reflection of the k-th arch across the line $s = s_k$ gives an arch lying under the $(k-1)$-st arch (i.e., $|v(s_k + t)| \leqq |v(s_k - t)|$ for $0 \leqq t \leqq s_{k+1} - s_k$ and $s_{k+1} - s_k \leqq s_k - s_{k-1}$); cf. [4], p. 531 and p. 538. Thus if $f \in M_{10}$, the "alternating series argument" implies that (5.7) is convergent and non-negative for $t > 0$.

The kernel $G(t, s)$, for $s \geqq t$, can be written in the form

$$G(t,s) = v_1(t)v_2(s) - v_1(s)v_2(t), \tag{7.1}$$

where $v = v_1(s), v_2(s)$ are arbitrary solutions of (5.5) subject to the Wronskian condition

$$v_1(s)v_2'(s) - v_1'(s)v_2(s) \equiv 1. \tag{7.2}$$

Also, for fixed t,

$$G_t(t,s) = v_1'(t)v_2(s) - v_1(s)v_2'(t) \tag{7.3}$$

is a linear combination of $v_1(s), v_2(s)$ and is, therefore, a solution of (5.5). Hence, the integral in (5.9) is convergent (for the same reasons as is the integral in (5.7)).

If the upper limit of integration ∞ is replaced by a fixed T, it is seen that (5.7) and (5.9) represent a solution of (5.4) and its derivative. Thus the same is true for (5.7), (5.9) if it is verified that the integrals are uniformly convergent on compact t-sets of $t > 0$.

By the alternating series argument, the remainder $\left|\int_T^\infty\right|$ of the integral in (5.7) or (5.9) is majorized by $C(b-a)f(T)$, where $s=a, b$ are successive zeros of $v(s)=G(t,s)$ or $v(s)=G_t(t,s)$, $a \leqq T \leqq b$, and $|G|$ or $|G_t|$ is majorized by C for $s \geqq t$. The monotony of q implies that $b-a \leqq \pi/q^{\frac{1}{2}}(t)$. By (5.10), $v(s)=G(t,s)$ is such that $V=v^2+v'^2/q$ is non-increasing for $s>t$. Hence $v^2(s) \leqq V(s) \leqq V(t)$ for $s \geqq t > T_0$. Thus

$$(7.4) \qquad |G(t,s)|^2 \leqq |G_s(t,t)|^2/q(t) = 1/q(t) \text{ for } s \geqq t > T_0.$$

Similarly (cf. (5.8)),

$$(7.5) \qquad |G_t(t,s)|^2 \leqq |G_t(t,t)|^2 = 1 \text{ for } s \geqq t > T_0.$$

Hence C can be chosen to be $1/q^{\frac{1}{2}}(t)$, 1 in the respective cases of (5.7), (5.9). Thus the remainder $\left|\int_T^\infty\right|$ is at most $\pi f(T)/q(t)$ or $\pi f(T)/q^{\frac{1}{2}}(t)$ in the cases (5.7) or (5.9). This proves the uniform convergence of (5.7), (5.9) on compact subsets of $t>0$.

This argument (with $T=t$) also shows that if $t>T_0$, then

$$(7.6) \qquad 0 \leqq w(t) \leqq \pi f(t)/q(t), \qquad |w'(t)| \leqq \pi f(t)/q^{\frac{1}{2}}(t).$$

Hence $w, w' \to 0$ as $t \to \infty$. Also $w''=-qw+f$ satisfies $|w''| \leqq (\pi+1)f(t) \to 0$ as $t \to \infty$. This proves Theorem 6.1_0.

8. Proof of Theorem 6.1_1. In order to prove $w'(t) \leqq 0$ for $t>0$, consider first only $t>T_0$ and write (5.9) as

$$(8.1) \qquad w'(t)=\int_t^\infty [G_t(t,s)q(s)][f(s)/q(s)]ds.$$

Since $v(s)=G_t(t,s)$ is a solution of (5.5), it follows that $G_t(t,s)q(s) = -G_{tss}(t,s)$. An integration by parts applied to (8.1) gives

$$w'(t)=-G_{ts}(t,s)f(s)/q(s)]_{s=t}^{s=\infty}+\int_t^\infty G_{ts}(t,s)\,(f/q)'ds.$$

The integrated terms vanish for, on the one hand, (7.3) show that $G_{ts}(t,t) = 0$, and, on the other hand, $G_{ts}(t,s)/q^{\frac{1}{2}}(s), 1/q^{\frac{1}{2}}(s)=O(1)$ and $f(s) \to 0$ as $s \to \infty$. (The boundedness of $G_{ts}(t,s)/q^{\frac{1}{2}}(s)$ follows from the non-increasing character of $v^2+v'^2/q$, where $v(s)=G_t(t,s)$; cf. (5.10).)

Another integration by parts gives

$$w'(t)=(G_s(t,s)+1)\,(f(s)/q(s))']_{s=t}^{s=\infty}-\int_t^\infty [G_t(t,s)+1]\,(f/q)''ds.$$

The integrated term at $s=t$ vanishes for $G_t(t,t)+1=0$ by (7.2), (7.3).

The term at $s=\infty$ is also 0 for $v(s)=G_t(t,s)$ is bounded and $(f/q)'\rightarrow 0$ as $s\rightarrow\infty$. (The last limit relation follows from the fact that $(f/q)'$ is monotone and integrable over $t\leqq s<\infty$.) Thus

$$w'(t)=-\int_t^\infty [G_t(t,s)+1](f(s)/q(s))''ds. \tag{8.2}$$

The assumptions on f,q imply that $(f/q)''\geqq 0$ for $s\geqq T_0$. The factor $G_t(t,s)+1\geqq 0$ by (7.5). Thus $w'(t)\leqq 0$ for $t>T_0$.

In order to deal with $w'(t)$ on the interval $0<t\leqq T_0$, when $T_0>0$, note that if a solution of (5.4) (i.e., $w''=-qw+f$) satisfies initial conditions $w(T_0)>0$, $w'(T_0)<0$, then $q\leqq 0$ and $f\geqq 0$ imply, for reasons of convexity, that $w(t)\geqq 0$, $w'(t)\leqq 0$, $w''(t)\geqq 0$ for $0<t\leqq T_0$. By continuity, the same holds for initial conditions $w(T_0)\geqq 0$, $w'(T_0)\leqq 0$. Hence $w'(t)\leqq 0$ for $0<t\leqq T_0$.

It remains to show that $w'''(t)\rightarrow 0$ as $t\rightarrow\infty$. Note that the first factor in the integrand in (8.2) satisfies $|G_t(t,s)+1|\leqq 2$ for $t>T_0$, by (7.5). Hence (8.2) implies that

$$0\leqq -w'(t)\leqq -2(f(t)/q(t))' \text{ for } t>T_0. \tag{8.3}$$

Thus, the first inequality in (7.6) can be improved to

$$0\leqq w(t)\leqq 2f(t)/q(t) \text{ for } t>T_0. \tag{8.4}$$

By (8.3) and the boundedness of q',

$$0\leqq -qw'\leqq -2f'+2fq'/q\rightarrow 0 \text{ as } t\rightarrow\infty. \tag{8.5}$$

Thus a differentiation of (5.4) shows that

$$w'''=-qw'-q'w+f'\rightarrow 0 \text{ as } t\rightarrow\infty. \tag{8.6}$$

This proves Theorem 6.1_1.

9. Proof of Theorem 6.1_2. It will first be shown that $w''(t)\geqq 0$. If $q\leqq 0$ for $0<t\leqq T_0$, then $w''=-qw+f\geqq 0$ for $0<t\leqq T_0$. Thus, it can be supposed that $t>T_0$ and that $q(t)>0$ on this t-range. Dividing (5.4) by q and differentiating twice gives

$$W''+qW=(f/q)'', \text{ where } W=w''/q. \tag{9.1}$$

Since q satisfies the conditions of Theorem 6.1_2, hence Theorem 6.1_0, and $(f/q)''\in M_{1,0}(T_0,\infty)$, it follows from Theorem 6.1_0 that (9.1) has a non-negative solution for $t>T_0$ given by

$$W(t)=\int_t^\infty G(t,s)(f/q)''ds$$

satisfying $W, W', W'' \to 0$ as $t \to \infty$. By uniqueness (cf. Remark 1 following the statement of Theorem 6.1_n), this solution is $W = w''/q$, where w is given by (5.7).

(Note that under the conditions of Theorem 6.1_2, the inequality in (8.4) can be improved to

$$0 \leqq w(t) \leqq f(t)/q(t) \text{ for } t > T_0. \tag{9.2}$$

This is clear from the inequality $w'' = f - qw \geqq 0$.)

It remains to show that $w^{(4)}(t) \to 0$ as $t \to \infty$. Let (5.4) be differentiated to give

$$w''' + qw' = f' - q'w. \tag{9.3}$$

The function $-(f' - q'w)$ is of class $M_{2,0}(T_0, \infty)$. Thus, by Theorem 6.1_1, equation (9.3) considered as a second order, inhomogeneous equation for w' has a unique solution, the negative of which is class $M_{1,3}(T_0, \infty)$. Since uniqueness refers to the class of solutions satisfying $(w')' \to 0$ as $t \to \infty$, this solution is the derivative of (5.7). Thus $-w' \in M_{1,3}$ and $w \geqq 0$, that is, $w \in M_{2,4}$. This proves Theorem 6.1_2.

10. Proof of Theorem 6.2_0. Since $v(s) = G(t,s)$ is a solution of (5.5), $G(t,s) = -G_{ss}(t,s)/q(s)$. Thus, without considering questions of convergence, the integral in (5.7) can be written formally as

$$w(t) = -\int_t^\infty G_{ss}(t,s) f(s)\, ds/q(s). \tag{10.1}$$

An integration by parts gives

$$w(t) = (1 - G_s(t,s))(f(s)/q(s))]_{s=t}^{s=\infty} - \int_t^\infty [1 - G_s(t,s)](f/q)' ds. \tag{10.2}$$

The integrated term at $s = t$ vanishes since $1 - G_s(t,t) = 0$ by (6.2). Since q is non-increasing, (5.11) shows that $V = qv^2 + v'^2$ is non-increasing if $v(s) = G(t,s)$. In particular, $v'^2(s) \leqq V(s) \leqq V(t) = 1$ for $s \geqq t$ and so, $|G_s(t,s)| \leqq 1$. Thus

$$0 \leqq 1 - G_s(t,s) \leqq 2 \text{ for } s \geqq t. \tag{10.3}$$

Since $f/q \to 0$ and $s \to \infty$, the integrated term at $s = \infty$ in (10.2) is 0. Since $(f/q)' \leqq 0$ and is (absolutely) integrable over $t \leqq s < \infty$, it follows that the integral in (10.1) is convergent and

$$w(t) = -\int_t^\infty [1 - G_s(t,s)](f(s)/q(s))' ds. \tag{10.4}$$

In fact, the integral in (10.1) is uniformly convergent on compact subsets of $t > 0$.

Since $1 - G_s(t, s) = 0$ if $s = t$, differentiation of (10.4) gives

$$w'(t) = \int_t^\infty G_{ts}(t, s)\,(f(s)/q(s))'ds. \tag{10.5}$$

This interchange of differentiation and integration is valid for the monotony of q and (5.11) imply that

$$|G_{ts}(t, s)| \leqq q^{\frac{1}{2}}(t) \leqq \text{const. for } s \geqq t. \tag{10.6}$$

It is now readily verified that (5.7) represents a solution of (5.4). Also (10.3) and (10.4) show that $w(t) \geqq 0$ and

$$0 \leqq w(t) \leqq 2f(t)/q(t) \text{ for } t > 0. \tag{10.7}$$

Also, (10.5) and (10.6) give

$$|w'(t)| \leqq f(t)/q^{\frac{1}{2}}(t) \text{ for } t > 0. \tag{10.8}$$

These facts imply the assertions of Theorem 6.2_0, namely, $w(t) \geqq 0$ and $w, w', w'' \rightarrow 0$ as $t \rightarrow \infty$.

11. Proof of Theorem 6.2_n, $n > 0$. Dividing (5.4) by q and differentiating gives

$$(w''/q)' + w' = (f/q)'. \tag{11.1}$$

On introducing the new variables W, τ defined by

$$W = -w' \text{ and } d\tau = q(t)\,dt \tag{11.2}$$

(11.1) can be written as

$$D^2W + (1/q)W = -D(f/q), \text{ where } D = d/d\tau = q^{-1}(t)\,d/dt. \tag{11.3}$$

Note that $(1/q^2)' = 2D(1/q)$. Thus an assumption of Theorem 6.2_n implies that $D(1/q) \in DM_n$. Since $n > 0$, $D(1/q) \geqq 0$ and $D^2(1/q) \leqq 0$, as a function of τ, $1/q$ is non-decreasing and concave. Since (11.3) is oscillatory at the upper end of the τ-range, it follows that $\tau(t)$ satisfies $\tau(\infty) = \infty$. Thus, $0 < t < \infty$ is mapped onto some range $(-\infty \leqq)T^0 < \tau < \infty$.

The assumptions of Theorem 6.2_n imply that, as functions of τ, $1/q$ and $-D(f/q)$ satisfy the assumptions of Theorem 6.1_{n-1}. Hence, (11.3) has a unique solution $W = W(t)$ of class $DM_{n-1,n+1}$.

Uniqueness refers to the class of solutions satisfying $DW \rightarrow 0$ as $t \rightarrow \infty$. According to the last section (11.2), the function w given by (5.7) is such that $W = -w'$ is a solution of (11.3). Also, $DW = -w''/q = w - f/q \to 0$ as $t \to \infty$. Thus, if $w(t)$ is defined by (5.7), then $W = -w' \in DM_{n-1,n+1}$. This proves Theorem 6.2_n.

Part III. Differential equations of higher order.

12. Statement of results. The object of this part of the paper is to obtain analogues of Theorem 6.1_n for differential equations of the form

$$w^{(k+2)} + q(t)w^{(k)} - \sum_{j=0}^{k-1} (-1)^{j+k} g_j(t) w^{(j)} = (-1)^k f(t) \tag{12.1}$$

and for related non-linear equations of order $k + 2$.

THEOREM 12.1_n. *Let $n \geqq 0$. Let $q(t)$ posssess a derivative $q'(t)$ of class M_n and $0 < q(\infty) \leqq \infty$. Let $f(t) \in M_{n+1,0}$. If $k \geqq 1$, assume*

$$\int^{\infty} t^{k-1} f(t)\, dt/q(t) < \infty, \tag{12.2}$$

$g_j(t) \in M_{n+1}$, and

$$\int^{\infty} t^{k-j-1} g_j(t)\, dt/q(t) < \infty \quad for\ j = 0, \cdots, k-1. \tag{12.3}$$

Then (12.1) has a unique solution $w = w(t)$ of class $M_{n+k,n+k+2}$.

Remark 1. If, in addition, $g_0(\infty) = 0$ and c is a positive constant, then (12.1) has a unique solution $w = w(t)$ such that $w - c \in M_{n+k,n+k+2}$. This follows by introducing $w - c$ as a new dependent variabile in (12.1).

Remark 2. If all solutions of (5.5) tend to 0 as $t \to \infty$, then the conditions $f(\infty) = 0$ in Theorem 12.1_n and the condition $g_0(\infty) = 0$ in the last remark can be omitted except for assertion $w^{(k)} \to 0$ when $n = 0$.

Remark 3. If there is a $T_0 > 0$ such that $q(t) \leqq 0$ for $0 < t < T_0$ and $q(t) > 0$ for $t > T_0$, the conditions on q, f, g_j can be reduced on the interval $0 < t < T$ corresponding to Remark 3 following Theorem 6.1_n: for $n = 1, 2$, it is sufficient to require only $q \leqq 0$, $f \geqq 0$, $g_j \geqq 0$; for $n > 2$, it is sufficient to require that $q', f, g_j \in M_{n-2}(0, T_0)$.

Theorem 12.1_n and its Corollary should be contrasted with analogous theorems in [5], Appendix, in which it is assumed that $f \equiv 0$ and that $v'' + q(s)v = 0$ is disconjugate (rather than oscillatory) for $s > 0$, but no conditions like (12.2)-(12.3) occur.

Remark 4. It should be noted that neither of the conditions (12.2), (12.3) can be omitted in Theorem 12.1_n for any n (if $k \geqq 1$).

In order to see this, consider first the differential equation

$$w''' + w' = -1/(t+1),$$

where $k = 1$, $q = 1$, $g = 0$ and $f = (t+1)^{-1}$. All conditions of Theorem 12.1_n hold for every n except (12.2). If $w = w(t)$ is a solution for which $w' \leqq 0$, then

$$w'(t) = -\int_t^\infty (s+1)^{-1} \sin(s-t)\, ds,$$

by the Remark 1 following Theorem 6.1_n. It is easily seen, from an integration by parts, that $w'(t) = -t^{-1} + O(t^{-2})$ as $t \to \infty$. Hence $w(t) \to -\infty$ as $t \to \infty$. Consequently, (12.2) cannot be omitted in Theorem 12.1_n.

The differential equation

$$w''' + w' + Cw/t \log t = -2\epsilon/t \log^2 t, \tag{12.4}$$

where $C > 1$ and $\epsilon > 0$, satisfies all conditions of Theorem 12.1_n for every n except (12.3) if $t > 0$ is replaced by $t > 2$. If this equation has a solution $w = w(t)$ of class $M_1(2, \infty)$, then its derivative satisfies

$$\begin{aligned} -w' = 2\epsilon \int_t^\infty & \sin(s-t)\, ds/s \log^2 s \\ & + C \int_t^\infty w(s) \sin(s-t)\, ds/s \log s. \end{aligned} \tag{12.5}$$

Let T be so large that $t \geqq T$ implies the inequality

$$C \int_t^\infty \sin(s-t)\, ds/s \log^2 s \geqq 1/t \log^2 t$$

and the inequality which results if C is replaced by 2ϵ and the 1 on the right by ϵ. Then, since the last term of (12.5) is non-negative, $-w' \geqq \epsilon/t \log^2 t$ for $t \geqq T$. Hence $w = \epsilon/t \log t +$ (a non-negative, non-increasing function). Thus (12.5) implies $-w' \geqq 2\epsilon/t \log^2 t$ and so, $w(t) = 2\epsilon/t \log t +$ (a non-negative, non-increasing function). Continuing this argument, one obtains the contradiction $w(t) \geqq m\epsilon/t \log t$ for $t \geqq T$ and $m = 1, 2, \cdots$.

Actually, conditions (12.2), (12.3) can be lightened somewhat.

THEOREM 12.2_n. *Let $q, g_0, \cdots, g_{k-1}, f$ satisfy the conditions of Theorem 12.1_n except that (12.2)-(12.3) is replaced by the following when $k \geqq 1$: There exist positive, continuous functions $\epsilon_1(t), \cdots, \epsilon_k(t)$ for large t with the properties that, as $t \to \infty$,*

$$\int_t^\infty s^{m-1}q^{-1}(s)f(s)\,ds = O(\epsilon_m(t)), \tag{12.6}$$

$$\sum_{j=0}^{k-1}\int_t^\infty s^{m-1}q^{-1}(s)g_j(s)\epsilon_{k-j}(s)\,ds = o(\epsilon_m(t)), \tag{12.7}$$

for $m=1,\cdots,k$. *Then* (12.1) *has a unique solution* $w=w(t)$ *of class* $M_{n+k,n+k+2}$ *satisfying* $w^{(j)}(t)=O(\epsilon_{k-j}(t))$ *as* $t\to\infty$ *for* $j=0,\cdots,k-1$.

When (12.2)-(12.3) hold, then (12.6)-(12.7) are satisfied by $\epsilon_j(t)=1/t^{k-j}$ for $j=1,\cdots,k$. Also, if $w=w(t)$ is any function of class M_k, then $w^{(j)}(t)=O(1/t^{k-j})$ as $t\to\infty$ for $j=0,\cdots,k-1$. Thus Theorem 12.2_n is contained in Theorem 12.3_n.

Remark 5. On the one hand, Theorem 12.2_n becomes false if "$o(\epsilon_m(t))$" in (12.7) is replaced by "$O(\epsilon_m(t))$." This can be seen from the example (12.4) where $k=1$, $q=1$, $g_0=C/t\log t$ and $f=2\epsilon/t\log^2 t$, so that the integral in (12.7) is majorized by $C\epsilon_1(t)$ if $\epsilon_1(t)=1/\log t$. On the other hand, (12.6)-(12.7) can be weakened to

$$\gamma_n\int_t^\infty (s-t)^{m-1}q^{-1}(s)f(s)\,ds \leqq (1-\theta)\epsilon_m(t), \tag{12.8}$$

$$\int_t^\infty (s-t)^{m-1}G(s)\,ds \leqq \theta\epsilon_m(t), \tag{12.9}$$

for $t\geqq T$ and $m=1,\cdots,k$, where $0<\theta<1$, T is some (fixed) positive number,

$$G(s)=\gamma_n q^{-1}(s)\sum_{j=0}^{k-1} g_j(s)\epsilon_{k-j}(s)/(k-j-1)!, \tag{12.10}$$

$\gamma_0=\pi$, $\gamma_1=2$ and $\gamma_n=1$ for $n\geqq 2$. It is clear that (12.6)-(12.7) imply (12.8)-(12.9) if $\epsilon_m(t)$ is replaced by (const.)$\epsilon_m(t)$ for a suitable constant. The factor $\gamma_n=1$ in (12.9)-(12.10) for $n\geqq 2$ cannot be replaced by a smaller constant (even when the constant implicit in the O-term of (12.6) is arbitrarily small). For example, (12.4) has a completely monotone solution if $\epsilon>0$ and $0\leqq C<1$, but it has no non-negative, non-increasing solution if $\epsilon>0$, $C>1$.

Remark 6. Under the assumptions of Theorem 12.2_n, (12.1) can have more than one solution of class $M_{n+k,n+k+2}$. For Theorem 20.1_n below implies that the differential equation (18.2) has a non-trivial solution $w=w(t)\not\equiv 0$, as well as the trivial solution $w\equiv 0$, of class $M_{n+1,n+3}$. In (18.2), where $k=1$, $f=0$ and $q(\infty)=\infty$, the function $\epsilon_1(t)=e^{-t}$ satisfies (12.7) since $q'/q\to 0$, $t\to\infty$.

Theorem 12.2_n has an analogue for non-linear equations of the form

(12.11) $$w^{(k+2)} + q(t)w^{(k)} = (-1)^k F(t, w, -w', \cdots, (-1)^{k-1}w^{(k-1)}).$$

Introduce the abbreviations

(12.12) $$f(t) = F(t, 0, \cdots, 0)$$

and, if $F = F(t, \alpha_0, \cdots, \alpha_{k-1})$,

(12.13) $g_j(t) = \partial F/\partial\alpha_j$ at $\alpha_i = \epsilon_{k-i}(t)/(k-i-1)!$ for $j = 0, 1, \cdots, k-1$.

THEOREM 12.3_n. *Let $q(t)$ be as in Theorem 12.1_n and $q(t) > 0$ for $t > 0$. Let $F(t, \alpha_0, \cdots, \alpha_{k-1})$ be defined for $t > 0$, $\alpha_i \geqq 0$ and have continuous partial derivatives satisfying*

(12.14) $$(-1)^m \partial^{m+h+i+\cdots+j} F/\partial t^m \partial\alpha_0{}^h \partial\alpha_1{}^i \cdots \partial\alpha_{k-1}{}^j \geqq 0$$

for $m \leqq n+1$ and $m+h+i+\cdots+j \leqq n+2$; let

(12.15) $$F(t, \alpha_0, \cdots, \alpha_{k-1}) \to 0 \text{ as } (t, \alpha_0, \cdots, \alpha_{k-1}) \to (\infty, 0, \cdots, 0);$$

finally, let there exist positive continuous functions $\epsilon_1(t), \cdots, \epsilon_k(t)$ for $t > 0$ and a constant θ, $0 < \theta < 1$, such that (12.12), (12.13), (12.10) *satisfy* (12.8), (12.9) *for $t > 0$ and $m = 1, \cdots, k$. Then* (12.10) *has a unique solution $w = w(t)$ of class $M_{n+k,n+k+2}$ satisfying $(-1)^j w^{(j)}(t) \leqq \epsilon_{k-j}(t)/(k-j)!$ for $t > 0$ and $j = 0, \cdots, k-1$.*

Combining Theorems 12.1_n, 12.2_n or 12.3_n with the theorem of Hausdorff-Bernstein gives

COROLLARY. *If the conditions of Theorem 12.1_n [or 12.2_n or 12.3_n] are satisfied for $n = 0, 1, \cdots$, then* (12.1) [*or* (12.1) *or* (12.11)] *has a unique [or at least one] solution $w = w(t)$ representable in the form*

$$w(t) = \int_0^\infty e^{-st} d\sigma(s) \text{ for } t > 0, \text{ where } d\sigma \geqq 0.$$

If, in addition, to the conditions of Theorem 12.1_n, $g_0(\infty) = 0$ and $c > 0$, then (12.1) *has a unique solution representable in the form*

$$w(t) = c + \int_0^\infty e^{-st} d\sigma(s) \text{ for } t > 0, \text{ where } d\sigma \geqq 0.$$

The existence statement of Theorems 12.2_n and 12.3_n, for the cases $n = 0, 1, 2$, will be proved in Section 13, the uniqueness statement in Section 14. This will be used to prove Theorem 6.1_n for $n > 2$, first for the case

$q(\infty) < \infty$ in Section 15 and then for the case $q(\infty) = \infty$ in Section 16. These results, in turn, will be used to complete the proof of Theorems 12. 2_n and 12. 3_n. $n > 2$, in Section 17.

13. Existence in Theorems 12. 2_n and 12. 3_n, $n \leqq 2$. In this section, it will be supposed that $n = 0$, 1, or 2. If $k = 0$, the assertion to be proved is contained in Theorem 6. 1_n. Suppose therefore that $k \geqq 1$.

In order to deal with Theorems 12. 2_n and 12. 3_n at the same time, let (12.1) be written in the form (12.11). For the proof of Thetorem 12. 3_n, it will be supposed that T is any positive number; for Theorem 12. 2_n, it will be supposed that T is so large that $q(t) > 0$ and (12.8), (12.9) hold for $t \geqq T$.

The desired solution will be obtained by successive approximations. Let $w_0 \equiv 0$. If $w_m(t)$ have been defined, put

$$(13.1_m) \qquad f_m(t) = F(t, w_m(t), -w_m'(t), \cdots, (-1)^{k-1} w_m^{(k-1)}(t)).$$

If possible, define the k-th derivative of w_{m+1} by

$$(13.2_m) \qquad w_{m+1}^{(k)}(t) = (-1)^k \int_t^\infty G(t,s) f_m(s)\, ds$$

and the lower order derivatives by

$$(13.3_m) \qquad w_{m+1}^{(j)}(t) = (-1)^{k-j} \int_t^\infty (s-t)^{k-j-1} w_{m+1}^{(k)}(s)\, ds/(k-j-1)!$$

for $j = 0, \cdots, k-1$. Thus, formally

$$(13.4_m) \qquad w_{m+1}^{(k+2)} + q w_{m+1}^{(k)} = (-1)^k f_m.$$

It will be shown, by induction on m, that $w_0 \equiv 0$ and (13.1)-(13.4) define a sequence of functions $w_0, w_1, \cdots$ satisfying

$$(13.5_m) \qquad w_m \in M_{n+k,n+k+2}, \qquad f_m \in M_{n+1,0},$$

in fact, $\Delta w_m = w_m - w_{m-1}$ satisfies

$$(13.6_m) \qquad \Delta w_{m+1} \in M_{n+k,n+k+2},$$

$$(13.7_m) \quad (-1)^j \Delta w_{m+1}^{(j)} \leqq (1-\theta)\theta^m \epsilon_{k-j}(t)/(k-j-1)! \text{ for } t \geqq T,$$
$$j = 0, 1, \cdots, k-1.$$

Note that, by (13.1_m) and (12.14),

$$(13.8) \qquad w_m \in M_{n+k,n+k+2} \text{ implies } f_m \in M_{n+1,0}.$$

If w_m, w_{m+1} have been defined and $\Delta f_m = f_m - f_{m-1}$, then

$$\Delta f_{m+1}(t) = \sum_{j=0}^{k-1} (-1)^j \left(\int_0^1 F_j{}^0 d\tau \right) \Delta w_{m+1}{}^{(j)}(t), \tag{13.9}$$

where $F_j = \partial F / \partial \alpha_j$ and

$$\begin{aligned} F_j{}^0(t,\tau) = F_j(t, [\tau w_{m+1}(t) + (1-\tau) w_m], \\ \cdots, (-1)^{k-1}[\tau w_{m+1}{}^{(k-1)}(t) + (1-\tau) w_m{}^{(k-1)}(t)]). \end{aligned} \tag{13.10}$$

Thus, by (12.14),

(13.11) $\qquad$ (13.5_m), (13.5_{m+1}), (13.6_m) imply $\Delta f_{m+1} \in M_{n+1,0}$.

If (13.7_0), $\cdot \cdot \cdot$, (13.7_m) hold, then

$$(-1)^j w_{m+1}{}^{(j)} \leqq (1-\theta) \sum_{i=0}^{m} \theta^m \epsilon_{k-j}/(k-j-1)! \leqq \epsilon_{k-j}/(k-j-1)!.$$

Also, if $(-1)^j \Delta w_{m+1}{}^{(j)} \geqq 0$, then

$$(-1)^j [\tau w_{m+1}{}^{(j)} + (1-\tau) w_m{}^{(j)}] \leqq (-1)^j w_{m+1}{}^{(j)} \text{ for } 0 \leqq \tau \leqq 1.$$

Thus, by (13.9), (12.13) and (12.10),

(13.12) $\qquad$ (13.6_m) and (13.7_0), $\cdot \cdot \cdot$, (13.7_m) imply (13.13_m),

where

$$\gamma_n \Delta f_{m+1}/q \leqq (1-\theta)\theta^m G \text{ for } t \geqq T. \tag{13.13_m}$$

If w_{m-1}, w_m have been defined for some $m \geqq 1$, then the k-th derivative of w_{m+1} or, equivalently, of Δw_{m+1} will be defined by the use of

$$\Delta w_{m+1}{}^{(k+2)} + q \Delta w_{m+1}{}^{(k)} = (-1)^k \Delta f_m. \tag{13.14}$$

If (13.5_{m-1}), (13.5_m) and (13.6_{m-1}) hold, so that $\Delta f_m \in M_{n+1,0}$ by (13.11), then (13.14) considered as a second order equation for $\Delta w_{m+1}{}^{(k)}$ has, according to Theorem 6.1_n, a unique solution such that $(-1)^k \Delta w_{m+1}{}^{(k)} \in M_{n,n+2}$ and

$$\Delta w_{m+1}{}^{(k)} = (-1)^k \int_t^\infty G(t,s) \Delta f_m(s)\, ds. \tag{13.15}$$

Also, the remark concerning (6.3) shows that for $t \geqq T$,

$$| \Delta w_{m+1}{}^{(k)} | \leqq \gamma_n \Delta f_m / q, \qquad | \Delta w_{m+1}{}^{(k)\prime} | \leqq \pi \Delta f_m / q^{\frac{1}{2}}. \tag{13.16}$$

If, in addition, (13.13_{m-1}) holds, then the integrals in

$$\begin{aligned} &\Delta w_{m+1}{}^{(j)}(t) \\ &\qquad = (-1)^{k-j} \int_t^\infty (s-t)^{k-j-1} \Delta w_{m+1}{}^{(k)}(s)\, ds/(k-j-1)! \end{aligned} \tag{13.17}$$

for $j=0,\cdots,k-1$ are convergent and serve to define a function Δw_{m+1} such that $d^k(\Delta_{m+1})/dt^k=\Delta w_{m+1}{}^{(k)}$, so that $\Delta w_{m+1}\in M_{n+k,n+k+2}$. Also, (13.13_{m-1}) implies

$$(13.18_m)\qquad (-1)^k\Delta w_{m+1}{}^{(k)}\leqq(1-\theta)\theta^{m-1}G \text{ for } t\geqq T,\ m>0,$$

$$(13.19_m)\qquad |\Delta w_{m+1}{}^{(k+1)}|\leqq(\pi/\gamma_n)(1-\theta)\theta^{m-1}q^{\frac{1}{2}}G \text{ for } t\geqq T,\ m>0.$$

By (12.9) and (13.17), the inequality (13.18_m) implies (13.7_m). Summarizing this paragraph,

(13.20) (13.5_{m-1}), (13.5_m), (13.6_{m-1}),
(13.13_{m-1}) imply (13.5_{m+1}), (13.6_m), (13.7_m).

It follows from (13.8), (13.12) and (13.20) that, in order to prove the existence of the sequence $w_0\equiv 0, w_1,\cdots$ satisfying (13.5)-(13.7), it is sufficient to verify the existence of w_1 such that w_1 and $\Delta w_1=w_1-w_0=w_1$ satisfy (13.5_1), (13.6_0) and (13.7_0).

It is clear from (12.14)-(12.15) and $f_0=F(t,0,\cdots,0)$ that $f_0\in M_{n+1,0}$. Hence, by Theorem 6.1_n, (13.4_0) has a unique solution $w_1{}^{(k)}$ given by (13.2_0) and $(-1)^k w_1{}^{(k)}\in M_{n,n+2}$. Also, by (6.3) and the remarks about it,

$$(13.21)\qquad 0\leqq(-1)^k w_1{}^{(k)}\leqq\gamma_n f_0/q,\qquad |w_1{}^{(k)\prime}|\leqq\pi f_0/q^{\frac{1}{2}}$$

for $t\geqq T$. Thus (12.8), where $f=f_0$, shows that (13.3_0) is meaningful for $j=0,\cdots,k-1$ and defines a function $w_1\in M_{n+k,n+k+1}$ with $d^k w_1/dt^k=w_1{}^{(k)}$. Also, (13.3_0) and (12.8) imply (13.7_0). This complete the induction.

Consequently, $w^{(j)}(t)=\lim w_m{}^{(j)}(t)$, as $m\to\infty$, exist uniformly for $j=0,\cdots,k+1$ (hence, for $j=k+2,\cdots,k+n+2$ also) on compact subsets of $t\geqq T$. It follows that the limit function $w=w(t)$ is a solution of (12.11) for $t\geqq T$, is of class $M_{n+k}(T,\infty)$, and satisfies

$$(13.22)\qquad (-1)^j w^{(j)}(t)\leqq\epsilon_{k-j}(t)/(k-j-1)! \text{ for } t\geqq T,\ j=0,\cdots,k-1.$$

Also, by (13.18_m) for $m\geqq 1$ and (13.21)

$$(13.23)\qquad (-1)^k w_m{}^{(k)}(t)\leqq G(t)+\gamma_n f_0(t)/q(t) \text{ for } m\geqq 0.$$

Thus, by Lebesgue's theorem on majorized convergence, it follows that, one can let m tend to ∞ in (13.3_m). In particular, (13.22) can be sharpened to

$$(-1)^j w^{(j)}(t)\leqq(-1)^k\int_t^\infty(s-t)^{k-j-1}[G(s)+\gamma_n f_0(s)/q(s)]ds/(k-j-1)!,$$

so that $w^{(j)}\to 0$ as $t\to\infty$ for $j=0,\cdots,k-1$. By (12.4) and (12.15), $F(t,w(t),\cdots,(-1)^{k-1}w^{(k-1)}(t))\in M_{n+1,0}(T,\infty)$. Thus if (12.11) is considered as a second order equation for $w^{(k)}$, it follows from Theorem 6.1_n that $(-1)^k w^k \in M_{n,n+2}(T,\infty)$, hence $w \in M_{n+k,n+k+2}(T,\infty)$.

Since $T > 0$ is arbitrary for Theorem 12.3_n, the existence statement [illegible] that theorem $(n \leqq 2)$ is proved.

In order to complete the proof of the existence statement in Theorem 12.2_n, $n \leqq 2$, it is sufficient to verify the uniform convergence of the approximations $w_m(t)$ and their derivatives on closed subintervals of $0 < t \leqq T$. For the remainder of this section, assume that (12.11) is the equation (12.1) and that $0 < t_0 \leqq t \leqq T$.

By (13.13_{m-1}) and (13.15), it follows there exists a constant $C = C(t_0)$ such that

$$|\Delta w_{m+1}{}^{(k)}| \leqq C\{\int_t^T |\Delta f_m(s)|\, ds + \theta\} \text{ for } m \geqq 1; \tag{13.24}$$

cf. the remarks following (7.5) for the estimate of $\int_T^\infty$ in (13.15). Repeated integrations of (13.24) over the interval (t, T) and (13.7) give

$$\begin{aligned} &|\Delta w_{m+1}{}^{(k-j)}| \\ &\leqq C\{\int_t^T (s-t)^{j-1} |\Delta f_m(s)|\, ds/(j-1)! + \theta^m \sum_{i=0}^{j} (T-t)^i/i!\}, \end{aligned} \tag{13.25}$$

for $j = 1, \cdots, k-1$ if C is sufficiently large. Thus, by (13.9),

$$\begin{aligned} &|\Delta f_{m+1}| \\ &\leqq C\{\int_T^t \sum_{j=0}^{k-1} (s-t)^{j-1} |\Delta f_m(s)|\, ds/(j-1)! + \theta^m \sum_{j=0}^{k-1} (T-t)^j/j!\}. \end{aligned} \tag{13.26}$$

In (13.26), $C = C(t_0)$ is a sufficiently large constant (independent of m). The existence of C depends on the linearity of (12.1), so that $F_j{}^0$ in (13.9) is merely the coefficient function $g_j(t)$ in (12.1) and hence has a bound for $t_0 \leqq t \leqq T$ independent of m.

An induction on m shows that

$$|\Delta f_{m+1}| \leqq C \sum_{i=0}^{m-1} \theta^{m-1-i} (Ck)^i \sum_{j=i}^{\infty} (T-t)^j/j! \tag{13.27}$$

for $m \geqq 1$. Thus,

$$\sum_{m=1}^{\infty} |\Delta f_{m+1}| \leqq C(\sum_{i=0}^{\infty} \theta^i)(\sum_{i=0}^{\infty} (Ck)^i \sum_{j=i}^{\infty} (T-t_0)^j/j!) < \infty.$$

In view of (13.24)-(13.25), it follows that $w^{(j)} = \lim w_m{}^{(j)}$ exists uniformly for $0 < t_0 \leqq t \leqq T$ if $j = 0, \cdots, k$. Since an inequality similar to (13.24) holds for $\Delta w_{m+1}{}^{(k+1)}$, the uniform limit relation is valid for $j = k+1$; hence,

$+ 2, \cdots, n + k + 2$ also. This completes the existence proof in $. 2_n$, $n \leqq 2$.

14. Uniqueness in Theorems 12. 2_n and 12. 3_n. The uniqueness assertion for $n = 0$ implies uniqueness for $n \geqq 0$. Thus it will be supposed that $n = 0$. In view of Theorem 6. 1_0, it can be supposed that $k \geqq 1$.

Let $w = w(t)$ be the solution of (12.11) just constructed in the last section. Suppose that $w = W(t)$ is another solution with the stated properties. If $W(t)$ is compared with the 0-th approximations $w_0 = 0$, it is seen that the case $m = 0$ of

$$(14.1) \qquad (-1)^j (W^{(j)} - w_m^{(j)}) \geqq 0 \text{ for } j = 0, \cdots, k$$

holds. An induction shows the validity of (14.1) for $m = 0, 1, \cdots$. Thus

$$(14.2) \qquad (-1)^j (W^{(j)} - w^{(j)}) \geqq 0 \text{ for } j = 0, \cdots, k.$$

Let T be so large that (13.22) holds and that the analogous inequalities hold for $w = W(t)$. Let

$$(14.3) \qquad \Delta w_m = W - w_m$$

and

$$(14.4) \quad \Delta f_m = F(t, W, \cdots, (-1)^{k-1} W^{k-1}) - F(t, w_m, \cdots, (-1)^{k-1} w_m^{(k-1)}).$$

Then, the case $m = 0$ of

$$(14.5) \quad (-1)^j \Delta w_m^{(j)} \leqq \theta^m \epsilon_{k-j}(t)/(k-j-1)! \text{ for } t \geqq T,\ j = 0, \cdots, k-1$$

holds. On repeating the arguments leading to (13.7_m), it is seen that (14.5) holds for $m \geqq 0$. Hence, $W - w = \lim \Delta w_m$, as $m \to \infty$, is 0 for $t \geqq T$. Since $W - w$ is a solution of a linear, homogenous differential equation for $t > 0$, it follows that $W - w = 0$ for $t > 0$. This proves the uniqueness assertion.

15. Proof of Theorem 6. 1_n, $q(\infty) < \infty$. Let $n > 2$ and $0 < q(\infty) < \infty$ in the statement of Theorem 6. 1_n. Let the differential equation (5.4) be differentiated $n - 2$ times to give

$$(15.1) \qquad w^{(n)} + q w^{(n-2)} + \sum_{j=0}^{n-3} C_{n-2,j} q^{(n-2-j)} w^{(j)} = f^{(n-2)}.$$

If this equation is identified with (12.1), then $k = n - 2$,

$$g_j = (-1)^{j+n-1} C_{n-2,j} q^{(n-2-j)}$$

and the f on the right side of (12.1) is $(-1)^{n-2}f^{(n-2)}$. The assumptio Theorem 6.1_n imply those of Theorem 12.1_2 for q and that g_j, $(-1)^{n-}$ $\in M_{2+1,0}$. Clearly, condition (12.2) holds, and (12.3) hold when $q(\infty) < \infty$.

Since Theorem 12.2_2, has been proved, it follows that (15.1) has a unique solution $w = w(t) \in M_{n,n+2}$. Successive integrations of (15.1) show that $w = w(t)$ satisfies

$$w'' + qw = f + P_{n-3}(t), \tag{15.2}$$

where $P_{n-3}(t)$ is a polynomial of degree $n-3$. But since $q(\infty) < \infty$, $w \in M_{n,n+2}$ imply $w'', qw, f \to 0$ as $t \to \infty$, it follows that $P_{n-3}(t) = 0$. Hence, $w = w(t)$ is a solution of (5.4) with the desired properties. The uniqueness of this solution follows from the uniqueness of solutions of class $M_{n,n+2}$ for (15.1).

16. Proof of Theorem 6.1$_n$. It remains to prove the cases of Theorem 6.1_n, where $n > 2$ and $q(\infty) = \infty$.

By assumption, $q' \in M_n$. Hence $(-1)^{j+1}q^{(j)} \geqq 0$ for $j = 1, \cdots, n+1$ and $q^{(j)}(\infty) = 0$ for $j = 1, \cdots, n$. There exists a sequence of functions $h_1, h_2, \cdots$ on $t > 0$, such that $0 \leqq (-1)^n h_1 \leqq (-1)^n h_2 \leqq \cdots \leqq (-1)^n q^{(n+1)}$, $h_m \equiv 0$ for large t, and $q^{(n+1)}(t) = \lim h_m(t)$, as $m \to \infty$, uniformly on compact subsets of $t > 0$. Define $q_m(t)$ on $t > 0$ by

$$q_m^{(n+1)}(t) = h_m(t), \quad q_m^{(j)}(\infty) = 0 \text{ for } j = 1, \cdots, n \text{ and } q_m(1) = q(1);$$

so that, in particular,

$$q_m^{(j)}(t) = (-1)^{n-j+1}\int_t^\infty (s-t)^{n-j}h_m(s)\,ds/(n-j)! \text{ for } j = 1, \cdots, n$$

and $q_m' \in M_n$, $q_m(\infty) < \infty$. It is clear that $(-1)^{j+1}q_m^{(j)} \leqq (-1)^{j+1}q^{(j)}$ for $j = 1, \cdots, n+1$ and $t > 0$. Also

$$q_m^{(j)} \to q^{(j)} \text{ as } m \to \infty \tag{16.1}$$

uniformly on compact subsets of $t > 0$ for $j = 0, \cdots, n+1$. In particular, after discarding a finite number of q_m, if necessary, it can be supposed that $q_m(\infty) > 0$.

By the cases of Theorem 6.1_n already proved, it follows that

$$w'' + q_m w = f \tag{16.2}$$

has a unique solution $w = w_m(t)$ of class $M_{n,n+2}$. If $G_m(t,s)$ is the Green's function belonging to (16.2), then

$$w_m(t) = \int_t^\infty G_m(t,s)f(s)\,ds. \tag{16.3}$$

By the proof of Theorem 6.1_0 in Section 7, $q_m(t) > 0$ for $t \geqq T$ implies

$$(16.4) \qquad \left| \int_T^\infty G_m(t,s) f(s)\, ds \right| \leqq \pi f(T)/q_m(t).$$

It is clear from the uniformity of (16.1) for $j = 0$ that $G_m(t,s) \to G(t,s)$, $m \to \infty$, uniformly on compact subsets of $s \geqq t > 0$. Hence (16.3), (16.4) imply that $w_m(t) \to w(t)$, $m \to \infty$, uniformly on compact subsets of $t > 0$; hence $w = w(t)$ is the solution (5.7) of (5.4). Similarly, it is shown that $w_m'(t) \to w'(t)$, $m \to \infty$, uniformly on compact subsets of $t > 0$.

It then follows from the differential equations (5.4), (16.2) and from (16.1) that $w_m^{(j)} \to w^{(j)}$, $m \to \infty$, uniformly on compact subsets of $t > 0$ for $j = 0, \cdots, n+3$. Thus $w_m \in M_n$ for $m = 1, 2, \cdots$ implies that $w \in M_n$. Since $w \in M_{0,2}$ by Theorem 6.1_0, $w \in M_{n,n-1}$. Let (5.4) be differentiated $n-2$ times,

$$(16.5) \qquad w^{(n)} + q(t) w^{(n-2)} = -\sum_{j=0}^{n-3} C_{n-2,j} q^{(n-2-j)} w^{(j)} + f^{(n-2)}.$$

If the right side of (16.5) is multiplied by $(-1)^{n-2}$, it becomes a function of class $M_{3,0}$. Thus, considering (16.5) as an inhomogeneous differential equation of second order for $w^{(n-2)}$ with known right side, Theorem 6.1_2 implies that there is a unique solution $w^{(n-2)} = w^{(n-2)}(t)$ such that $(-1)^{n-2} w^{(n-2)} \in M_{2,4}$. Uniqueness refers to the class of solutions satisfying $(w^{(n-2)})' \to 0$ as $t \to \infty$. Thus this solution $w^{(n-2)} = w^{(n-2)}(t)$ is the $(n-2)$-nd derivative of (5.7). Hence $w \in M_{n,n+2}$.

17. Proof of Theorems 12.2_n and 12.3_n, completed. In view of Sections 13 and 16, it can be supposed that $k \geqq 1$ and $n > 2$. Let $w_0 \equiv 0$, $w_1, \cdots$ be the sequence of successive approximations defined in Section 13. By virtue of Theorem 6.1_n, $n > 2$, proved in the last section, and a simple induction, it is seen that the m-th approximation w_m is of class $M_{n+k,n+k+2}$ for $m = 0, 1, \cdots$. Furthermore, the convergences of the sequences $\{w_m\}$, $\{w_m'\}$, $\cdots$, $\{w_m^{(k+1)}\}$ proved in Section 13 implies the convergence of the sequences $\{w_m^{(k+2)}\}, \cdots, \{w_m^{(k+n+2)}\}$. Consequently $w_m \in M_{n+k}$ for $m = 0, 1, \cdots$ implies that $w = \lim w_m$ is of class M_{n+k}. Since $w \in M_{n+2,0}$ by Theorems 12.2_2 or 12.3_2, it follows that $w \in M_{n+k,n+k+1}$.

Differentiating (12.1) or (12.11) $n-2$ times and applying an argument similar to that at the end of the last section shows that $w \in M_{n+k,n+k+2}$.

Part IV. Higher order monotony of $|z|^2$.

18. The differential equation of Appell. It was remarked by Appell ([1]; cf. [10], p. 298) that to a linear, homogeneous, second order differential equation, say $L_2u = 0$, there corresponds a linear, homogeneous, third order, differential equation $L_3w = 0$ such that if $u = x(t), y(t)$ are arbitrary solutions of $L_2u = 0$, then $w = x(t)y(t)$ is a solution of $L_3w = 0$. When $L_2u = 0$ is of the form

$$u'' + q(t)u = 0, \tag{18.1}$$

then $L_3w = 0$ is given by

$$w''' + 4q(t)w' + 2q'(t)w = 0. \tag{18.2}$$

An application of Theorem 12.1_n (and Remark 1) to (18.2) gives

THEOREM 18.1_n. *Let $n \geqq 0$. Let $q(t)$ possess a derivative $q'(t)$ of class M_{n+1} and $0 < q(\infty) < \infty$. Then* (18.1) *has a pair of solutions $u = x(t), y(t)$ such that*

$$w = x^2(t) + y^2(t) > 0 \tag{18.3}$$

satisfies

$$w(t) - 1 \in M_{n+1,n+3}. \tag{18.4}$$

(*The pair of solutions (x, y) of* (18.1) *in* (18.3) *is unique up to their replacement by $(ax + by, cx + dy)$, where a, b, c, d are constants such that $a^2 + c^2 = b^2 + d^2 = 1$, $ab + cd = 0$.*)

A corollary of this assertion and the theorem of Hausdorff-Bernstein is

COROLLARY. *Let $q(t)$ possess a derivative $q'(t)$ of class M_n for $n = 1, 2, \cdots$ and $0 < q(\infty) < \infty$. Then* (18.1) *has a pair of solutions $u = x(t), y(t)$ such that* (18.3) *has a representation of the form*

$$w(t) = 1 + \int_0^\infty e^{-ts} d\sigma(s) \text{ for } t > 0 \tag{18.5}$$

with a non-decreasing weight function $\sigma = \sigma(s)$.

19. Proof of Theorem 18.1_n. Let $u = u_1(t)$, $u_2(t)$ be linearly independent solutions of (18.1). Then the general solution of (18.2) is a linear combination of u_1^2, u_1u_2, u_2^2. It follows that if $w = w(t)$ is any solution of (18.2), then $w(t)$ can be written either in the form $w = \pm[x^2(t) + y^2(t)]$

or in the form $w = x^2(t) - y^2(t)$, where $u = x(t), y(t)$ are (possibly trivial) solution of (18.1).

The conditions of Theorem 18.1_n imply that (18.2) satisfies the conditions of Theorem 12.1_n, where $k = 1$, q is replaced by $4q$, $g_0(\mathrm{t}) = 2q'(t)$ and $f(t) = 0$. Since $q(\infty) < \infty$, the derivative $q'(t)$ is integrable over $1 \leqq t < \infty$. Hence the monotony of q' implies $g_0(\infty) = 0$. Thus, Theorem 12.1_n and the Remark 1 following it imply that (18.2) has a unique solution $w = w(t)$ satisfying (18.4). Because of the oscillatory nature of the solution of (18.1), this $w(t)$ must be of the form (18.3), where $u = x, y$ are linearly independent solutions of (18.1).

The uniqueness of the solution $w = w(t)$ of (18.2) implies the uniqueness of x, y as specified. For the identity $x^2 + y^2 = (ax + by)^2 + (cx + dy)^2$ and the linear independence of the solutions $w = x^2, xy, y^2$ of (18.2) imply the given relations between the constants a, b, c, d.

20. The case $q(\infty) = \infty$. Theorem 18.1_n and its Corollary have analogues in the case $q(t) \to \infty$ as $t \to \infty$.

THEOREM 20.1_n. *Let* $n \geqq 0$. *Let* $q(t)$ *possess a derivative* $q'(t)$ *of class* M_{n+1} *and* $q(\infty) = \infty$. *Then* (18.1) *has a pair solutions* $u = x(t), y(t)$ *such that* (18.3) *satisfies*

$$(20.1) \qquad w(t) \in M_{n+1,n+3}.$$

(*The uniqueness assertion of Theorem* 18.1_n *is valid.*)

The analogue of the Corollary of Theorem 18.1_n is

COROLLARY. *Let* $q(t)$ *possess a derivative* $q'(t)$ *of class* M_n *for* $n = 1, 2, \cdots$ *and* $q(\infty) = \infty$. *Then* (18.1) *has a pair of solutions* $u = x(t), y(t)$ *such that* (18.3) *has a representation as a Laplace-Stieltjes integral*

$$(20.2) \qquad w(t) = \int_0^\infty e^{-st} d\sigma(s) \text{ for } t > 0$$

with a non-decreasing weight function $\sigma = \sigma(s)$.

21. Proof of Theorem 20.1_n. The use of the Riemann-Liouville change of variables (2.7) in (18.1) leads to the differential equation (1.2), where Q is given by (2.1). Note that $Q - 1 \geqq 0$ and

$$\int^\infty (Q-1)\, ds = \int^\infty (Q-1) q^{\frac{1}{2}}\, dt < \infty.$$

Thus, by a theorem of Bôcher (cf. [12], p. 261), (1.2) has a pair of solution $U = X(s), Y(s)$ which satisfy, in terms of the s-variable, as $s \rightarrow \infty$,

$$X(s) = \cos s + o(1), \qquad dX/ds = -\sin s + o(1),$$
$$Y(s) = \sin s + o(1), \qquad dY/d(s) = \cos s + o(1).$$

If $x(t) = q^{-\frac{1}{4}}(t)X(s)$, $y(t) = q^{-\frac{1}{4}}(t)Y(s)$ are the corresponding solutions of (18.1), then the boundedness of q' and $ds = q^{\frac{1}{2}}\,dt$ imply that, as $t \rightarrow \infty$,

$$\begin{aligned} x(t) &= q^{-\frac{1}{4}}(t)(\cos s + o(1)), \qquad & x'(t) &= q^{\frac{1}{4}}(t)(-\sin s + o(1)), \\ y(t) &= q^{-\frac{1}{4}}(t)(\sin s + o(1)), \qquad & y'(t) &= q^{\frac{1}{4}}(t)(\cos s + o(1)), \end{aligned} \tag{21.1}$$

where $s = s(t) \rightarrow \infty$ as $t \rightarrow \infty$.

Consider the general solution $w = w(t)$ of (18.2),

$$w = ax^2 + bxy + cy^2$$

which can be written in the form

$$w = a[x^2 + y^2] + [bx + (c - a)y]y. \tag{21.2}$$

Thus, by (21.1), the derivative satisfies

$$w' = ao(1) + A[\sin(2s + \theta) + o(1)], \tag{21.3}$$

where $\theta = \theta(a, b, c)$ is a constant,

$$A = [b^2 + (c - a)^2]^{\frac{1}{2}} \geqq 0, \tag{21.4}$$

and the $o(1)$ terms have a monotone majorant, say, $\epsilon(t) \rightarrow 0$ as $t \rightarrow \infty$, independent of a, b, c. It follows that if T is large and $w'(t)$ does not change signs on the interval $\frac{1}{2}T \leqq t \leqq T$, then

$$a \neq 0 \text{ and } 0 \leqq A \leqq |a| \, \epsilon(\tfrac{1}{2}T). \tag{21.5}$$

Suppose that for every large $T > 0$, there exists a function $q_T = q_T(t)$ on $t > 0$ with the properties that $q_T(t) \equiv q(t)$ for $0 < t \leqq T$ and that $q_T(t)$ satisfies the assumptions of Theorem 18.1_n (that is, q and q_T satisfy the same conditions except that $0 < q_T(\infty) < \infty$ while $q(\infty) = \infty$).

By Theorem 18.1_n,

$$v'' + q_T(t)v = 0 \tag{21.6}$$

has a pair of solutions $v = x_T(t), y_T(t)$ such that $w_T = x_T{}^2 + y_T{}^2$ satisfies $w_T(t) - 1 \in M_{n+1,n+3}$. On $0 < t < T$, $v = x_T(t), y_T(t)$ are solutions of (18.1) and so, w_T is of the form (21.2) on this interval. In particular, (21.2) is of class $M_{n+1}(0,T)$ and, hence, (21.5) holds. After (21.2) is multiplied by a suitable positive constant, it can be supposed that $a=\pm 1$ and that (21.2) is of class $M_{n+1}(0,T)$.

In order to show the dependence on T, rewrite (21.2) as

$$w=w_T(t)=a_Tx^2+b_Txy+c_Ty^2,\quad a_T=\pm 1. \tag{21.7}$$

Let T tend to ∞ through a sequence of values for which $a=\lim a_T=\pm 1$ exists. Then it is clear from (21.4), (21.5) that

$$\lim_{T\to\infty} w_T(t)=a(x^2+y^2) \tag{21.8}$$

and that this limit relation can be formally differentiated $n+3$ times. If $S>0$ is fixed, then $w_T\in M_{n+1}(0,S)$ if $T>S$. Hence $a=1$ and the limit function $w=x^2+y^2$ is of class $M_{n+1}(0,S)$ for every S, i.e., $w=x^2+y^2\in M_{n+1}$.

By (21.1), w and w' tend to 0 as $t\to\infty$. Hence, if (18.2) is considered as an inhomogeneous, second order equation

$$(-w')''+4q(t)(-w')=2q'(t)w(t)$$

for $-w'$, then the (known) right side is of class $M_{n+1,0}$. Hence, by Theorem 6.1_n, $-w'\in M_{n,n+2}$, that is, $w\in M_{n+1,n+3}$.

Thus, in order to complete the proof of Theorem 20.1_n, it remains to verify the existence of the function $q_T(t)$ with the stated properties. Let $T>0$ be large and fixed. Since it is desired that $q_T(t)\equiv q(t)$ for $0<t\leqq T$, it suffices to define $q_T(t)$ on $t\geqq T$ so that $q_T'\in M_{n+1}(T,\infty)$, $q_T^{(j)}(T)=q^{(j)}(T)$ for $j=0,\cdots,n+2$ and $q_T(\infty)<\infty$.

Note that for $j=1,\cdots,n+1$

$$q^{(j)}(T)=(-1)^{n+j}\int_T^\infty (s-T)^{n+1-j}q^{(n+2)}(s)\,ds/(n+1-j)! \tag{21.9}$$

or, equivalently, for $j=0,\cdots,n$,

$$(-1)^{n+j}(j!)\,q^{(n+1-j)}(T)=(-1)^{n+1}\int_0^\infty s^j\,dq^{(n+1)}(s+T). \tag{21.10}$$

But $q(\infty)=\infty$ implies

$$(-1)^{n+1}\int_0^\infty s^{n+1}\,dq^{(n+1)}(s+T)=\infty. \tag{21.11}$$

The relations (21.10) mean that the reduced moment problem for $j=0,\cdots,n$,

$$\mu_j=\int_0^\infty s^j\,d\psi(s), \tag{21.12}$$

where $\mu_j = (-1)^{n+j}(j!)q^{(n+1-j)}(T)$, has a non-decreasing (absolutely continuous) solution $\psi(s) = (-1)^{n+1}q^{(n+1)}(s+T)$ for $s \geqq 0$. It is then clear from the conditions for the solvability of the Stieltjes' moment problem ([8], p. 6), that the finite sequence $\mu_0, \cdots, \mu_n$ can be extended to an infinite sequence $\mu_0, \mu_1, \cdots$ for which there exists a non-decreasing function $\psi(s)$ on $s \geqq 0$ satisfying (21.12) for $j = 0, 1, \cdots$.

In terms of such a solution ψ, define for $j = 1, \cdots, n+1$ and $t \geqq T$,

$$q_T^{(j)}(t) = (-1)^{1+j}\int_t^\infty (s-t)^{n+1-j}\,d\psi(s)/(n+1-j)! \tag{21.13}$$

$$q_T(t) = q(T) + \int_T^\infty q_T'(s)\,ds. \tag{21.14}$$

It is clear from (21.10) and the definitions of $\mu_0, \cdots, \mu_n$ that this definition of $q_T(t)$ for $t \geqq T$ together with the relation $q_T(t) = q(t)$ for $0 < t \leqq T$ give a function $q_T(t)$ on $t > 0$ such that $q_T'(t)$ is of class M_{n-1} and $q_T(\infty) < \infty$. Since ψ may not be continuous, q_T need not have an $(n+1)$-st derivative. But it is clear that $(-1)^{n-1}q_T^{(n)}(t)$ is non-negative, non-increasing and convex. For the purposes of the proof of Theorem 20.1_n such a function $q_T(t)$ will suffice; cf. the remark following the Definition 6.1 of the class $M_n(a,b)$.

22. The case of non-increasing q.

If q is non-increasing, one has the following analogue of Theorem 20.1_n.

THEOREM 22.1_n. *Let $n \geqq 0$. Let $q(t)$ be non-increasing and let* (18.1) *be oscillatory at $t = \infty$; in particular, $q(t) > 0$. Let $1/q^2$ have a derivative of class DM_{n+1}. Then* (18.1) *has a pair of solutions $u = x(t), y(t)$ such that* (18.3) *satisfies*

$$w'(t) \in DM_{n,n+2} \tag{22.1}$$

and

$$w(t) \to 1 \text{ or } w(t) \to \infty, \text{ as } t \to \infty, \tag{22.2}$$

according as $q(\infty) > 0$ or $q(\infty) = 0$. (The uniqueness assertion of Theorem 18.1_n is valid.)

For the definition of the class DM_n, see Definition 6.3.

Proof of Theorem 22.1_n. Divide (18.1) by q and differentiate to obtain

$$(u''/q)' + u' = 0. \tag{22.3}$$

Introduce the new variables

$$U = u', \qquad d\tau = q(t)\,dt, \tag{22.4}$$

so that (22.3) becomes

$$D^2U + (1/q)U = 0, \text{ where } D = d/d\tau = (1/q)\,d/dt. \tag{22.5}$$

As in Section 11, it is seen that $0 < t < \infty$ is mapped onto $(-\infty \leqq) T^0 < \tau < \infty$ and that (22.5) satisfies the assumptions of Theorem 20.1_n.

Hence, (22.5) has a pair of solutions $U = X, Y$ such that

$$W = X^2 + Y^2 > 0 \tag{22.6}$$

and either

$$W - 1 \in DM_{n+1,n+3} \text{ or } W \in DM_{n+1,n+3} \tag{22.7}$$

according as $q(\infty) > 0$ or $q(\infty) = 0$. Let $u = x, y$ be the solutions of (18.1) satisfying $X = x'$, $Y = y'$; cf. (22.4). Note that $W = x'^2 + y'^2$ and that, by (18.1) and (18.3)

$$-DW = -(2/q)(x'x'' + y'y'') = 2(x'x + y'y) \equiv w'.$$

Hence, (22.1) follows from (22.7).

The assertion that $w(t) \to 1$ as $t \to \infty$ in the case $q(\infty) > 0$ can be proved by the argument at the beginning of Section 20 involving the Riemann-Liouville change of variables.

When q tends monotonously to 0 and (18.1) is oscillatory, (18.1) has at least one solution which is unbounded as $t \to \infty$; [4], p. 529(i). Hence $\limsup w(t) = \infty$ as $t \to \infty$. Since w is monotone by the case $n = 0$ of (22.1), it follows that $w(t) \to \infty$ as $t \to \infty$ in the case $q(\infty) = 0$.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] P. Appell, "Sur la transformations des équations différentielle linéaires," *Comptes Rendus* (Paris), vol. 91 (1880), pp. 211-214.

[2] P. Hartman, "On oscillators with large frequencies," ***Bolletino della Unione Matematica Italiana***, vol. (3) 14 (1959), pp. 62-65.

[3] ———, "On the existence of large or small solutions of linear differential equations," to appear.

[4] ——— and A. Wintner, "On non-conservative linear oscillators of low frequency," *American Journal of Mathematics*, vol. 70 (1948), pp. 529-539.

[5] ——— and A. Wintner, "Linear differential equations with completely monotone solutions," *ibid.*, vol. 76 (1954), pp. 199-206.

[6] ——— and A. Wintner, "On a problem of Poincaré concerning Riccati's equation," *ibid.*, vol. 77 (1955), pp. 791-804.

[7] P. Schafheitlin, "Die Lage der Nullstellen der Besselschen Funktionen zweiter Art," *Sitzungsberichte der Berliner Mathematischen Gesellschaft*, vol. 5 (1906), pp. 82-93.

[8] J. S. Shohat and J. D. Tamarkin, *The problem of moments*, New York (1943).

[9] G. N. Watson, *A treatise on the theory of Bessel functions*, 2nd ed., Cambridge (1958).

[10] ——— and E. T. Whittaker, *A course of modern analysis*, Cambridge (1940).

[11] A. Wintner, "On the normalization of characteristic differentials in continuous spectra," *The Physical Review*, vol. 72 (1947), pp. 516-517.

[12] ———, "Asymptotic integrations of the adiabatic oscillator," *American Journal of Mathematics*, vol. 69 (1947), pp. 251-272.

[13] ———, "On a principle of reciprocity between high- and low-frequency problems concerning linear differential equations of second order," *Quarterly of Applied Mathematics*, vol. 15 (1957), pp. 314-317.

SYMMETRIC PRODUCTS AND JACOBIANS.*[1]

By Arthur Mattuck.

The n-fold symmetric product $C(n)$ of an algebraic curve C is a variety closely related to the Jacobian variety J of the curve. The low symmetric products appear birationally as a family of subvarieties of J for which there is no good analogue on other abelian varieties and which have been used by Matsusaka to characterize Jacobians intrinsically among abelian varieties. The higher symmetric products are used to construct the Jacobian, either by the excisions-and-glue method of Weil, or the more precise projective method of Chow.

Now Chow's construction of the Jacobian as a quotient variety of $C(n)$ "fibered" by the linear systems [3] raises the question of whether $C(n)$, for $n > 2g - 2$, is actually an algebraic projective bundle over J. We have shown elsewhere [8] that this is so; it is thus natural to ask what the Chern classes (to speak somewhat loosely) of this bundle are. One of the objectives of this paper is to exhibit these clases as elements of $A(J)$, the rational equivalence ring of J. Once this is done, one has according to a theorem of Grothendieck the structure of $A(C(n))$ explicitly as an extension of $A(J)$. This gives for example in a natural form the structure of the homology rings of high symmetric products of the closed orientable topological surfaces, which have hitherto only been computed "in principle" by the use of Eilenberg-MacLane spaces.

As a by-product of this determination of Chern classes, we get certain intersection relations among the subvarieties of J alluded to above which can be thought of as generalizing to lower dimensions the well-known (and obvious) "relation" $\Theta = \Theta^*$; they express W_i^* in terms of W_i.

The intersection relations on $C(n)$ and J here given, in particular the basic formula of Section 7, have other applications. For example, they clarify and conceptually simplify the proofs of the intersection formulas for the W_i given by Weil and Matsusaka [7] which play the crucial role in the characterization of J by Matsusaka previously alluded to, also the formulas from

---

* Received September 26, 1960.

[1] This research was supported in part by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under contract no. AF 18(603)-90.

which Weil's original proof of the Riemann hypothesis was derived. Again, they can be used as the basis for a geometric account of the Weierstrass points, with generalizations. These will appear separately.

Part II of this paper is devoted to the Chern classes. Part I is preliminary, and has connection with theorems of Chow and Andreotti. In it we prove that if C is a non-hyperelliptic curve, then any $g-1$ points of a generic canonical divisor are algebraically independent (but as will be seen, only just!). In addition to being used in a critical argument of Part II, we also use it to squeeze out the dimension and irreducibility of certain subvarieties of $C(n)$ which play an important role in Part II, as well as in the other applications alluded to above.

Our emphasis throughout is on rational equivalence, not anything coarser.

0. Preliminaries and notation. We will work throughout over a fixed algebraically closed ground field k, and "generic" will always mean with respect to this field. All our basic varieties will be defined over k, and all points and divisors used in constructions unless specifically called generic, will be understood to be k-rational.

We denote by C a fixed projective (complete) non-singular curve over k. Then $C(n)$ is its n-fold symmetric product, a non-singular projective variety most conveniently defined by the Chow coordinates [3, p. 456]. Its points represent the positive divisors of degree n on C.

Except in Section 5, we shall reserve the word "divisor" exclusively for *non-negative zero-cycles on* C, and shall denote them by German letters $\mathfrak{a}, \mathfrak{b}, \cdots$. We will use a superscript to indicate their degree, wherever it is convenient in the argument to be reminded of it: thus $\mathfrak{a}$ and $\mathfrak{a}^r$ in the same context represent the same positive divisor of degree r. The dimension of a divisor, $\dim \mathfrak{a}$, always the geometric (projective) dimension of the complete linear system $|\mathfrak{a}|$ to which it belongs: so $\dim \mathfrak{a} = l(\mathfrak{a}) - 1$.

To avoid some tedious locutions, we shall often casually identify the point on $C(n)$ with the divisor of degree n it represents, and thus speak of "the point $\mathfrak{a}^n$ on $C(n)$." Where we wish to be precise, we shall use $p(\mathfrak{a})$ for this point. Latin letters $x, y, p, q, \cdots$ will be reserved exclusively for points on C; capital letters for varieties and cycles on them. Superscripts and subscripts on capital letters in general refer to dimension and codimension, so that on $C(n)$, X_i and X^{n-i} represent the same cycle. Where indices must be used to distinguish cycles, they will conform to this convention.

If X is a non-singular projective variety, by $A(X)$ we mean its rational equivalence ring graded by codimension, so that $A_i(X)$ is the group of cycle classes of codimension i. An important formula we shall use constantly in the second part is the *projection formula*: Let $f\colon V \to U$ be a regular map, where V is projective (more generally, let f be proper). If X is a cycle on U such that $f^{-1}(X)$ is defined as a cycle, and Y is a cycle on V such that $Y \cdot f^{-1}(X)$ is defined, then in the sense of maps on cycles,

$$f(Y \cdot f^{-1}(X)) = f(Y) \cdot X,$$

the right side being automatically defined.

Part I.

1. The independence property. Suppose fixed a linear system $\mathfrak{A}$ on the curve C, of degree n and dimension r (not necessarily complete), which we may think of as represented by the subvariety A^r on $C(n)$ associated with it; a generic divisor of $\mathfrak{A}$ is then by definition one corresponding to a generic point of A. Recall that a positive divisor $\mathfrak{b}$ is said to be *contained in* a divisor $\mathfrak{a}$ if $\mathfrak{a} \geqq \mathfrak{b}$; it is contained in $\mathfrak{A}$ if it is contained in some $\mathfrak{a} \in \mathfrak{A}$. What can be said about the totality of positive divisors of some fixed degree m contained in $\mathfrak{A}$? Their Chow points form a subset $A[m]$ of $C(m)$ about which we can say a little if we know that $\mathfrak{A}$ has the

Independence property. A linear system $\mathfrak{A}$ of dimension r will be said to have the independence property if any r points occurring in a generic divisor are independent generic points of C.

This notion has arisen incidentally in Chow's construction of the Jacobian [4], and in a weaker form (linear independence) in Andreotti's proof of Torelli's theorem [1, p. 813]. The property does not depend on the choice of generic divisor. We have then

THEOREM 1. *If the linear system $\mathfrak{A}$, of degree n and dimension r has the independence property, then*

(i) *$A[m]$ is a purely r-dimensional algebraic set on $C(m)$ if $m > r$, otherwise all of $C(m)$,*

(ii) *If $m \leqq r$, or nontrivially if $m \geqq n - r$, then $A[m]$ is even irreducible. This in particular will automatically be true (regardless of m) if $\mathfrak{A}$ is complete and either of degree $n > 2g - 2$, or the canonical system—always assuming it has the property.*

Proof. The points of $A[m]$ are those representing divisors $y_1 + \cdots + y_m$, where $y_1 + \cdots + y_m + \cdots + y_n \in \mathfrak{A}$ for suitable y_i $(i > m)$.

Let $\mathfrak{a} = x_1 + \cdots + x_n$ be a generic divisor of the system $\mathfrak{A}$. Then $\sum x_i \to \sum y_i$ is a specialization, since A^r is irreducible and $\mathfrak{a}$ is generic; an extension of the specialization to the x_i takes them in some order onto the y_i, so that $x_{i_1} + \cdots + x_{i_m} \to y_1 + \cdots + y_m$ is a specialization for some for some choice of the x_i. In other words, every divisor represented by a point of $A[m]$ is a specialization of at least one of the ${}_nC_m$ divisors $x_{j_1} + \cdots + x_{j_m}$ of degree m contained in $\mathfrak{a}$, and conversely, by similar reasoning it is clear that any specialization of one of these is represented by a point of $A[m]$.

Now by the independence property, any one of this finite number of divisors is either made up entirely of independent generic points (if $m \leqq r$) or contains r of them (if $m \geqq r$), hence the locus of its specializations is respectively either m-dimensional (and therefore all of $C(m)$) or r-dimensional. The union of these loci is as we have seen $A[m]$, which proves statement (i) of the theorem.

To show the irreducibility of $A[m]$ if $m \geqq n - r$, it being $C(m)$ if $m \leqq r$ and therefore trivially irreducible, what we clearly must show is that any two of the ${}_nC_m$ divisors $x_{j_1} + \cdots + x_{j_m}$ are specializations of each other. Let therefore $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be two such, so that

$$\mathfrak{a} = \mathfrak{a}_1 + \mathfrak{b}_1 = \mathfrak{a}_2 + \mathfrak{b}_2,$$

where the $\mathfrak{b}_i$ are positive divisors of degree $n - m$, which is $\leqq r$ by hypothesis. By the independence property the $\mathfrak{b}_i$ are each made up of $n - m$ independent generic points, so that there is a specialization $\mathfrak{b}_1 \to \mathfrak{b}_2$. Let $\mathfrak{a}_i'$ be a positive divisor of degree $r - (n - m)$ in $\mathfrak{a}_i$; then $\mathfrak{b}_i + \mathfrak{a}_i'$ is of degree r, has therefore only independent generic points, and so the specialization extends to $\mathfrak{b}_1 + \mathfrak{a}_1' \to \mathfrak{b}_2 + \mathfrak{a}_2'$. Extend it now to $\mathfrak{a}_1 + \mathfrak{b}_1 \to \mathfrak{c}$. Then $\mathfrak{c}$ is a divisor containing $\mathfrak{b}_2 + \mathfrak{a}_2'$ and it is also a divisor of $\mathfrak{A}$, since it is a specialization of the generic divisor $\mathfrak{a}$. Since A is of dimension r, and $\mathfrak{b}_2 + \mathfrak{a}_2'$ has r generic points, there can be only one divisor of $\mathfrak{a}$ containing $\mathfrak{b}_2 + \mathfrak{a}_2'$, so that $\mathfrak{c} = \mathfrak{a}$. We have therefore a specialization

$$\mathfrak{a}_1 + \mathfrak{b}_1 \to \mathfrak{c} = \mathfrak{a} = \mathfrak{a}_2 + \mathfrak{b}_2$$

extending $\mathfrak{b}_1 \to \mathfrak{b}_2$, so that $\mathfrak{a}_1 \to \mathfrak{a}_2$ is a specialization also, as was asserted.

As to the remaining statement, when will every positive m between 0 and r be either $\leqq r$ or $\geqq n - r$? If $n - r \leqq r + 1$, that is, if $n \leqq 2r + 1$. Now if the system $\mathfrak{A}$ is complete and of degree $n \geqq 2g - 1$, then by the Riemann-Roch theorem, $r = n - g$, so indeed $n \leqq 2(n - g) + 1$ while if $\mathfrak{A}$ is the canonical system, $n = 2g - 2$, $r = g - 1$, and $2g - 2 \leqq 2(g - 1) + 1$: we even have room to spare!

2. An independence criterion. The following criterion results from analysis of a proof of Chow [4].

A linear system $\mathfrak{A}$ *of dimension* r *has the independence property* $\Longleftrightarrow$ *for some choice of* $r-1$ *points* $y_1, \cdots, y_{r-1}$, *the linear system* $\mathfrak{A} - \sum y_i$ *has dimension one and no fixed points.*

Here $\mathfrak{A} - \sum y_i$ denotes the residual system (of degree $n-r+1$ if $\mathfrak{A}$ has degree n). Of course for general choice of the y_i the system will always have dimension one, but it may have fixed points.

Proof. Let $x_1 + \cdots + x_n$ be a generic divisor of $\mathfrak{A}$. Then the independence property is equivalent with the "generic" condition:

For every choice of $r-1$ independent generic points from among the x_i, the system $\mathfrak{A} - (x_{i_1} + \cdots + x_{i_{r-1}})$ has no fixed points.

Namely, this system is rational over $k(x_{i_1}, \cdots, x_{i_{r-1}})$, where k is a field of definition for C and $\mathfrak{A}$ over which the x_{i_k} are independent generic points, and it has $(x_1 + \cdots + x_n) - (x_{i_1} + \cdots + x_{i_{r-1}})$ as generic divisor. Thus a point of C is a fixed point of this system if and only if it is one of the remaining x_i and is algebraic over $k(x_{i_1}, \cdots, x_{i_{r-1}})$. Now if $\mathfrak{A}$ doesn't have the independence property, some r of the x_i are not independent, so we can indeed find such an algebraic x_{i_r}, and conversely the existence of such a situation means that $x_{i_1}, \cdots, x_{i_r}$ are not independent generic points, so that $\mathfrak{A}$ does not have the independence property.

This proves the forward implication of the criterion, since if $\mathfrak{A}$ has the property, one can take as the y_i just the points $x_{i_1}, \cdots, x_{i_{r-1}}$. The implication is reversed by showing first that $\mathfrak{A} - \sum x_{i_k} \to \mathfrak{A} - \sum y_k$ is a specialization (viewing say the linear systems as irreducible cycles on $C(n-r+1)$). From this the theorem follows, for if the latter system has no fixed points, neither does the former—for example if you consider a finite set $\{\mathfrak{b}_i\}$ of divisors without common point from the second system, then a set of foreimages $\{\mathfrak{a}_i\}$ for them in the first system also can have no common point.

So relabel the independent generic points $x_{i_1}, \cdots, x_{i_{r-1}}$ as $x_1, \cdots, x_{r-1}$. Make a specialization $(x_1, \cdots, x_{r-1}) \to (y_1, \cdots, y_{r-1})$ and extend it to $\mathfrak{A} - \sum x_i \to \mathfrak{B}$, where B will be a one-dimensional cycle on $C(n-r+1)$. We show the support of B coincides with the one dimensional system $\mathfrak{A} - \sum y_i$ (this is enough for our theorem) by showing its points all represent divisors of the latter system. Indeed, any such point represents a divisor $y_r + \cdots + y_n$ that is, over the preceding specializations, itself a specialization of the generic divisor $x_r + \cdots, + x_n$ of the first system. Thus $x_1 + \cdots + x_n \to y_1 + \cdots + y_n$

is a specialization extending the preceding ones. Now since $x_1 + \cdots + x_n \in \mathfrak{A}$, so does $y_1 + \cdots + y_n$, so that $y_r + \cdots + y_n \in \mathfrak{A} - (y_1 + \cdots + y_{r-1})$, as was asserted.

3. Applications of the criterion.

(a). The following is due to Chow [4]. *If $n > 2g$, then every complete system $\mathfrak{A}$ of degree n has the independence property.* Namely, the system has dimension $r = n - g$; let $x_1 + \cdots + x_n$ be a generic divisor, where the first r points are independent generic, and choose for the y_i the last $r - 1$ points. Then $\mathfrak{A} - \sum y_i = | x_1 + \cdots + x_{g+1} |$. But $n > 2g$ implies that $g + 1 \leqq r$, hence the $x_1, \cdots, x_{g+1}$ are independent generic and so this system has no fixed points, as required.

(b). THEOREM. *If C is not hyperelliptic, then the canonical system $\mathfrak{W}$ has the independence property.* Take the $y_1, \cdots, y_{g-2}$ to be independent generic points, so that $\dim \mathfrak{W} - \sum y_i = 1$. We have to show this system has no fixed point p. If it did, then $\dim \mathfrak{W} - \sum y_i - p = 1$, so that by the Riemann-Roch theorem, $\dim | \sum y_i + p | = 1$. This is impossible however, because it is known that [1] the special divisors on $C(g-1)$—those belonging to linear systems of positive dimension—lie on a closed set whose dimension is less than $g - 2$, and which therefore cannot contain the $g - 2$ dimensional point which represents $y_1 + \cdots + y_{g-2} + p$. [Briefly, one considers the canonical mapping of $C(g-1)$ onto projective $g - 1$ space defined by the g symmetric regular $g - 1$ forms on $C(g-1)$. If C is not hyperelliptic, this map fails to be defined exactly where these differentials all vanish—in the hyperelliptic case it is always defined—and by direct calculation this occurs exactly at those points of $C(g-1)$ representing special divisors. Since $C(g-1)$ is nonsingular, this fundamental locus for the map must be of dimension $\leqq g - 3$.]

This result is of course false if C is hyperelliptic.

(c). We do not need the following application in this paper, but have used it elsewhere to construct cross-sections of the projective bundle over the Jacobian [8].

PROPOSITION. *If $\mathfrak{A}$ is a complete linear system on C of degree $n > 2g$, or if $\mathfrak{A}$ is the canonical system and C is not hyperelliptic, then the rational map associated with $\mathfrak{A}$ is biregular, and the image C' is projectively normal.*

Proof. The rational map we mean is the one turning the divisors of A into hyperplane sections. Andreotti [1] has proved the second case of the theorem; we prove the first case similarly (it is the one used in [8]). If p_1 and p_2 are two distinct points on C, then by the Riemann-Roch theorem, $\dim \mathfrak{A} - p_1 > \dim \mathfrak{A} - p_1 - p_2$; thus there is a divisor through p_1 not passing through p_2, $\mathfrak{A}$ separates points, and the map is one-one. Biregularity follows from the projective normality of the image, and this in turn follows by showing the linear system $\mathfrak{L}_k$ of hypersurface sections of degree k is complete for all k, which we now do.

Let $\mathfrak{A}^{(k)}$ be the smallest linear system on C containing all divisors of the form $\mathfrak{a}_1 + \cdots + \mathfrak{a}_k$, $\mathfrak{a}_i$ in $\mathfrak{A}$. Clearly $\mathfrak{A}^{(k)} \subset \mathfrak{L}_k$; we show $\dim \mathfrak{A}^{(k)} \geqq nk - g$, which will prove $\mathfrak{A}^{(k)}$ and therefore also $\mathfrak{L}_k$ is complete.

By the independence property, say, a generic divisor of $\mathfrak{A}$ contains no repeated points. Let A and B be non-overlapping sets containing respectively $n - g - 1$ and g of these points. Since $n \geqq 2g + 1$, B has never more than $n - g - 1$ points (this many only when $n = 2g + 1$). Since $\mathfrak{A}$ has dimension $n - g$ and the independence property, we can pass hyperplanes H_1 and H_2 through A and B respectively, each containing no other points of $\mathfrak{a}$. Add to them hyperplanes $H_3, \cdots, H_{k+1}$ not passing through any points of $\mathfrak{a}$. Then $H_1 + \cdots + H_{k+1}$ is a hypersurface of degree $k + 1$ cutting out a divisor of $\mathfrak{A}^{(k+1)}$ and passing through the $n - 1$ points of $A + B$, but not the n points of $\mathfrak{a}$. Thus the n points of $\mathfrak{a}$ must impose independent conditions on $\mathfrak{A}^{(k+1)}$, which shows that $\dim \mathfrak{A}^{(k+1)} \geqq \dim \mathfrak{A}^{(k)} - n$; since $\dim \mathfrak{A}^{(1)} = n - g$, the argument is complete.

In the sequel an important role will be played by a set of varieties $S^{(i)}$, $i = -1, 0, 1, \cdots$, which we now define.

Definition. $S^{(i)}$ is the set of all points on $C(g+i)$ representing special divisors $\mathfrak{a}^{g+i}$: those for which $\dim |\mathfrak{a}| > i$.

THEOREM 2. *$S^{(i)}$ is a variety of dimension $g - 1$ for all $i = -1, \cdots, g - 2$, and otherwise empty.*

Proof. Exactly those divisors $\mathfrak{a}^{g+i}$ are special which are contained in the canonical system, for by the Riemann-Roch theorem,

$$\dim |\mathfrak{a}| > i \Longleftrightarrow \dim |\mathfrak{W} - \mathfrak{a}| \geqq 0 \Longleftrightarrow \mathfrak{w} \geqq \mathfrak{a} \text{ for some } \mathfrak{w} \in \mathfrak{W}.$$

If C is not hyperelliptic, by what we have proved, the canonical system has the independence property, and thus the result follows from Theorem 1.

If C is hyperelliptic, we must argue directly. There is then, by definition of hyperelliptic, a regular map $f\colon C \to P^1$ of C onto the projective line, of degree 2: that is, $[k(C) : k(P)] = 2$. The canonical system on C is composed of all divisors of the form $f^{-1}(x_1+\cdots+x_{g-1})$, where $\sum x_i$ runs over the complete linear system of all positive divisors of degree $g-1$ on P; namely, this is obviously a linear system, of degree $2g-2$ and dimension $g-1$, hence necessarily the canonical system.

Let now the $\{x_i\}$ be independent generic points, and let $f^{-1}(x_i)=y_i+y_i'$. Then the divisors of degree $g+i$ contained in the canonical system are all specializations of $y_1+\cdots+y_{g-1}+y_1'+\cdots+y_{i+1}'$: this is trivial to see, but tedious to write out. The point on $C(g+i)$ representing this divisor is thus a generic point for $S^{(i)}$, which is therefore irreducible and of dimension $g-1$.

Part II.

4. Some subvarieties of $C(n)$. To avoid confusion, in this section only we shall use $p(\mathfrak{a})$ for the point on $C(n)$ representing the divisor $\mathfrak{a}$ on the curve C.

There is a natural map

$$f\colon C(r)\times C(n-r)\to C(n), \qquad 1\leqq r\leqq n-1,$$

defined by $f[p(\mathfrak{a}^r),p(\mathfrak{b}^{n-r})]=p(\mathfrak{a}+\mathfrak{b})$. This map is regular, since it is single-valued and $C(r)\times C(n-r)$ is a normal variety. In fact, it is biregular on $p(\mathfrak{a}^r)\times C(n-r)$, as is easily seen.

We now define on $C(n)$ a subvariety denoted by $X[\mathfrak{a}]$ for all non-negative divisors $\mathfrak{a}$ as follows (ϕ denotes the empty set or divisor):

$$X[\phi]=C(n),\qquad X[\mathfrak{a}^n]=p(\mathfrak{a}),\qquad X[\mathfrak{a}^r]=\phi \text{ for } r>n,$$
$$X[\mathfrak{a}^r]=\text{image of } p(\mathfrak{a}^r)\times C\ (n-r) \text{ under } f\ (1\leqq r\leqq n-1).$$

Thus if $r<n$, then $X[\mathfrak{a}^r]$ is biregularly equivalent to $C(n-r)$.

We are interested here in the intersection relations of these subvarieties given by the next two propositions.

PROPOSITION 1. *If $\mathfrak{a}$ and $\mathfrak{b}$ have no common points, then $X[\mathfrak{a}]$ and $X[\mathfrak{b}]$ intersect properly on $C(n)$ and $X[\mathfrak{a}]\cdot X[\mathfrak{b}]=X[\mathfrak{a}+\mathfrak{b}]$.*

Proof. Set-theoretically we have under the assumptions evidently

$$X[\mathfrak{a}]\cap X[\mathfrak{b}]=X[\mathfrak{a}+\mathfrak{b}],$$

so that the intersection is proper. To show they intersect with multiplicity one, suppose first that $\mathfrak{a}$ and $\mathfrak{b}$ are independent generic divisors, so that neither $\mathfrak{a}$ nor $\mathfrak{b}$ has repeated points:

$$\mathfrak{a}=p_1+\cdots+p_r \text{ and } \mathfrak{b}=q_1+\cdots+q_s.$$

We use $C[n]$ to denote $C\times C\times\cdots\times C$ (n factors), and consider the obvious regular map of degree $n!$

$$g\colon C[n]\to C(n)$$

defined by $g(x_1,\cdots,x_n)=x_1+\cdots+x_n$. We claim first of all that

$$g^{-1}(X[\mathfrak{b}])=\sum\nolimits_\sigma q_1\times\cdots\times q_s\times C[n-s],$$

where the sum is over a set of $n!/(n-s)!$ permutations of the factors of $C[n]$ which make the summands on the right all distinct. In fact this relation is evidently true, set-theoretically, all coefficients must be the same for the summands on the right by reason of symmetry; if this coefficient is m, we have on applying g to the left side $n!X[\mathfrak{b}]$, and applying it to the right side

$$\begin{aligned}&m\sum\nolimits_\sigma g\sigma(q_1\times\cdots\times q_s\times C[n-s])\\&\qquad=\sum\nolimits_\sigma(n-s)!X[\mathfrak{b}]=m[n!/(n-s)!](n-s)!X[\mathfrak{b}],\end{aligned}$$

whence $m=1$.

Now putting $Y[\mathfrak{a}]=p_1\times\cdots\times p_r\times C[n-r]$ on $C[n]$, we have (assuming $r+s\leqq n$, and defining $C[0]=\phi$)

$$Y[\mathfrak{a}]\cdot g^{-1}(X[\mathfrak{b}])=p_1\times\cdots\times p_r\times(\sum\nolimits_\tau q_1\times\cdots\times q_s\times C[n-r-s]),$$

the sum taken over permutations τ which make the summands distinct. Applying g, we get therefore by the projection formula, since $g(Y[\mathfrak{a}])=(n-r)!X[\mathfrak{a}]$,

$$\begin{aligned}g(Y[\mathfrak{a}])\cdot X[\mathfrak{b}]&=(n-r)!X[\mathfrak{a}]\cdot X[\mathfrak{b}]\\&=[(n-r)!/(n-r-s)!](n-r-s)!X[\mathfrak{a}+\mathfrak{b}],\end{aligned}$$

so that our result $X[\mathfrak{a}]\cdot X[\mathfrak{b}]=X[\mathfrak{a}+\mathfrak{b}]$ is proved.

If now $\mathfrak{a}'$ and $\mathfrak{b}'$ are non-generic divisors, specialize $(\mathfrak{a},\mathfrak{b})\to(\mathfrak{a}',\mathfrak{b}')$; this extends uniquely in turn to

$$\mathfrak{a}+\mathfrak{b}\to\mathfrak{a}'+\mathfrak{b}',\quad \mathfrak{a}\times C(n-r)\to\mathfrak{a}'\times C(n-r),\quad X[\mathfrak{a}]\to X[\mathfrak{a}'],$$

and so on. Thus since the intersection of specialized positive cycles is the specialization of the intersection (if all intersections are proper), we get $X[\mathfrak{a}']\cdot X[\mathfrak{b}']=X[\mathfrak{a}'+\mathfrak{b}']$.

PROPOSITION 2. *Let $\xi[\mathfrak{a}]$ denote the rational equivalence class in $A(C(n))$ of $X[\mathfrak{a}]$. Then $\xi[\mathfrak{a}]\cdot\xi[\mathfrak{b}]=\xi[\mathfrak{a}+\mathfrak{b}]$.*

Proof. If $\mathfrak{a}^r$ and $\mathfrak{b}^s$ have no common points, this is just a weakening of Proposition one. If they do, find finite sets of divisors $\{\mathfrak{a}_i^r\}$ and $\{\mathfrak{a}_j'^r\}$ having no points in common with $\mathfrak{b}$ such that $p(\mathfrak{a})\sim\sum p(\mathfrak{a}_i)-\sum p(\mathfrak{a}'_j)$, the rational equivalence being on $C(r)$; it is a question only of avoiding certain subvarieties of $C(r)$ we shall not make explicit. Then

$$X[\mathfrak{a}] \sim \sum X[\mathfrak{a}_i] - \sum X[\mathfrak{a}_j']$$

on $C(n)$, since $X[\mathfrak{a}] = f(p(\mathfrak{a}) \times C(n-r))$ and rational equivalence is preserved by regular projective (proper) maps.

Now $\xi[\mathfrak{a}] \cdot \xi[\mathfrak{b}]$ is represented by

$$\sum X[\mathfrak{a}_i] \cdot X[\mathfrak{b}] - \sum X[\mathfrak{a}_j'] \cdot X[\mathfrak{b}] = \sum X[\mathfrak{a}_i + \mathfrak{b}] - \sum X[\mathfrak{a}_j' + \mathfrak{b}]$$
$$\sim X[\mathfrak{a} + \mathfrak{b}] \in \xi[\mathfrak{a} + \mathfrak{b}]$$

since $p(\mathfrak{a} + \mathfrak{b}) \sim \sum p(\mathfrak{a}_i + \mathfrak{b}) - \sum p(\mathfrak{a}_j' + \mathfrak{b})$ on $C(r+s)$, this being so because rational equivalence is preserved by the map of $C(r) \times C(s) \to C(r+s)$.

5. Chern classes of a projective bundle. As general references for what follows, see [5, 10].

Suppose that (E, X, π') is an algebraic vector bundle, that is, a fiber space in the sense of Andre Weil [12] whose fiber is a vector space V^p of dimension p. In other words, the base space should be a non-singular variety covered by open sets $\{U_i\}$ such that $\pi'^{-1}(U_i)$ is biregularly isomorphic to $V^p \times U$ by a fiber-preserving isomorphism (local triviality), and such that the transition functions $g'_{ij}\colon U_i \cap U_j \to \mathrm{GL}(p, k)$ are regular maps into the general linear group. We may then consider the derived algebraic projective bundle $(P(E), X, \pi)$, the points of whose fibers $\pi^{-1}(x)$ are the lines through the origin in the vector space $\pi'^{-1}(x)$. Formally it is given by the transition functions $g_{ij}\colon U_i \cap U_j \to \mathrm{PGL}(p-1, k)$ derived from the natural homomorphism: $\mathrm{GL}(p, k) \to \mathrm{PGL}(p-1, k)$. Since each point of $P(E)$ represents a line, $P(E)$ is the base space of a canonically determined line bundle whose dual bundle is denoted by L; associated with L is then a divisor class ξ in $A_1(P(E))$.

The natural map π^* is an isomorphism of $A(X)$ into $A(P(E))$; call its image $A(X)^*$ and write c^* for $\pi^*(c)$, if $c \in A(X)$. Then Grothendieck has proved that

$$A(P(E)) = A(X)^*[\xi],$$

where the minimal equation for ξ is:

$$\xi^p + c_1^* \xi^{p-1} + \cdots + c_p^* = 0.$$

The *Chern classes* of the vector bundle E are now defined to be the c_i, and $1 + c_1 + \cdots + c_p$ is called the *total Chern class* of E. Note also that it follows from Grothendieck's result that $A_1(P(E)) = A_0(X)^* \cdot \xi + A_1(X)^*$.

So far we have started with the vector bundle and derived ξ and the projective bundle from it. If we begin with a projective bundle, we may ask to what extent ξ in the above is uniquely determined (or even exists).

PROPOSITION 3. *An algebraic projective bundle* (F, X, π) *together with a given element* $\xi \in A_1(F)$ *is derived from a vector bundle* (E, X, π') *as described above if and only if* $\xi \cdot \pi^{-1}(x)$ *is the class of a hyperplane in the projective space* $\pi^{-1}(x)$, x *generic.*

Proof. For the necessity, since the restriction L' of L to a fiber $\pi^{-1}(x) = P^{p-1}$ is just the dual of the natural line bundle on P, we see that L' is associated with the divisor class of a hyperplane section of P, from which it follows that $\xi \cdot \pi^{-1}(x)$ is in $A(\pi^{-1}(x))$ the generating element represented by a hyperplane in $\pi^{-1}(x)$.

For the sufficiency, Grothendieck [6, § 3.4] has shown that an algebraic projective bundle is always derived from a vector bundle; suppose therefore that our bundle F is derived from (E_0, X, π') with $\xi_0 \in A_1(F)$ as associated divisor class, so that $\xi_0 \cdot \pi^{-1}(x)$ is the class of a hyperplane in $\pi^{-1}(x)$. If now $\xi \in A_1(F)$ is any other element with this property, it follows from the structure of the group $A_1(F)$ as given above that $\xi = \xi_0 + \lambda_1^*$, where $\lambda_1 \in A_1(X)$. Let L_1 be the line bundle on X associated with λ_1; then the vector bundle $E = E_0 \otimes L_1$ is the desired bundle: it has ξ as associated divisor, and E and E_0 have the same derived projective bundle, namely F.

Though this is all we need, for the sake of clarity we add a few remarks. It is easy to see that any vector bundle from which F is derived is of the form $E \otimes L_1$, where L_1 is a line bundle on X. If now X is complete, we get in this way a one-one correspondence between elements of $\xi + A_1(X)^*$ and vector bundles producing F. Now if ξ as above is a root of the polynomial $f(X) = \sum_0^p c_i^* X^{r-i}$, then $\xi + \lambda_1^*$ is a root of $f(X - \lambda_1^*) = \sum d_i^* X^{p-i}$, whose coefficients are polynomials in c_i and λ_1 (which are easily calculated) and in fact the Chern classes of $E \otimes L_1$. In other words, if we envision the elements $\lambda \in A_1(X)$ as acting on $A(X)$ as an additive group of automorphisms by

$$\lambda \colon 1 + c_1 + \cdots + c_n \rightarrow 1 + d_1 + \cdots + d_n \qquad (n = \dim X)$$

the d_i being determined as above, then what is an invariant of a projective bundle is the orbit of $\sum c_i$ under the group $A_1(X)$: the elements of the orbit are in 1-1 correspondence with the Chern classes of the vector bundles from which F is derived, and the orbit can reasonably be called the Chern class of F.

6. Statement of the result. We fix once and for all a point $p_0 \in C$. Then according to Section 4, we have a nested sequence of subvarieties of $C(n)$:

$$X[p_0] \supset X[2p_0] \supset \cdots \supset X[np_0]$$

which we shall abbreviate as $X_i = X[ip_0]$, so that X_i is of codimension i on $C(n)$. If we denote the rational equivalence class of X_1 by ξ, Proposition 2 shows that X_i represents the class $\xi^i = \xi \cdot \cdots \cdot \xi$ (i factors). Each X_i is biregularly isomorphic to $C(n-i)$.

Now let J be the Jacobian of C. Using our point p_0, we fix the canonical map $\phi\colon C \to J$ by making $\phi(p_0) = e$, the identity point of J. Then by linear extension of ϕ to divisors, we get a map

$$\pi\colon C(n) \to J.$$

We have proved elsewhere [8] that if $n > 2g-2$, which we shall henceforth assume, this triple $(C(n), J, \pi)$ is naturally a algebraic projective bundle whose fibers are the linear systems. On it we show now that the subvariety X_1 satisfies the hypotheses of Proposition 3: namely, for x generic on J, $X_1 \cdot \pi^{-1}(x)$ is in the rational equivalence class of a hyperplane on $\pi^{-1}(x)$. For the divisors making up $X_1 \cap \pi^{-1}(x)$ are those containing p_0; these form a linear subsystem of dimension $n-g-1$, in other words, a hyperplane in the projective space to which $\pi^{-1}(x)$ is biregularly equivalent. To see that the intersection multiplicity is one, it is enough to show that (using Proposition 1), $X[\mathfrak{a}^{n-g-1} + p_0] \cdot \pi^{-1}(x) = X[\mathfrak{a}] \cdot X_1 \cdot \pi^{-1}(x)$ consists of a single point with multiplicity one, if $\mathfrak{a}$ is "general." In fact, it consists of the divisors of $\pi^{-1}(x)$ containing $\mathfrak{a}^{n-g-1} + p_0$; it is well known that there is only one, and moreover, since the linear system represented by the points of $\pi^{-1}(x)$ is rational over $k(x)$ [3, p. 475], this unique divisor will be $k(x)$-rational and hence its representative point on $C(n)$ will be $k(x)$-rational too. Under these circumstances, the intersection multiplicity at the point is one.

It follows therefore that ξ, the rational equivalence class of X_1 in $A_1(C(n))$ is associated with a unique vector bundle E of rank $p = n - g + 1$ from which the bundle $C(n)$ is derived. We wish to compute the Chern classes of this bundle.

To this end, we let

$$W_i = \pi(X_{g+i})$$

so that W_i for $0 \leqq i < g$ consists of all points on J writable as $\phi(x_1) + \cdots + \phi(x_{g-i})$, and $W_g = e$, and $W_i = \phi$ for $i > g$. To eliminate asterisks, we also put

$$U_i = W_i^* = (W_i^-)_0,$$

that is, the transform of W_i by the biregular map of J sending x into $-x+c$, where $c=\pi(\mathfrak{k}^{2g-2}+(n-2g+2)p_0)$ is the canonical point on J.

THEOREM 3. *As a cycle on* $C(n)$, *we have*

$$X_p-\pi^{-1}(U_1)\cdot X_{p-1}+\pi^{-1}(U_2)\cdot X_{p-2}-\cdots+(-1)^g\pi^{-1}(U_g)\cdot X_{p-g}=0,$$
$$p=n-g+1.$$

Letting u_i be the rational equivalence class of U_i in $A_i(J)$ and using the fact that the class of X_i is ξ^i, we get immediately the

COROLLARY. *The total Chern class in* $A(J)$ *of the vector bundle* E *with derived projective bundle* $(C(n),J,\pi)$, $n>2g-2$, *and associated* $n-1$ *cycle* $X_1=X[p_0]$ *is*

$$1-u_1+u_2-\cdots+(-1)^g u_g.$$

7. Proof of Theorem 3. In what follows, in addition to viewing points of $C(n)$ as divisors on C without further comment, we shall often think of points on J as divisor classes of degree 0 on C. Thus for example $\pi(np_0)=e$ and $\pi(\mathfrak{a})=\mathrm{Cl}(\mathfrak{a}-np_0)$, where $\mathrm{Cl}(\mathfrak{a})$ means the divisor class to which $\mathfrak{a}$ belongs. For reference, we state explicitly,

(1) The divisors in X_i are those of the form $\mathfrak{a}^{n-i}+ip_0$.

(2) The classes in U_i are those containing a representative of the form $\mathfrak{k}-\mathfrak{a}^{g-i}-(g+i-2)p_0$ for some $\mathfrak{a}$ ($\mathfrak{k}$ is a canonical divisor).

An essential auxiliary role is played by the $g-1$ dimensional varities $S^{(i)}$ representing the special divisors on $C(g+i)$ that we introduced at the end of Part I. Under the biregular isomorphisms of $C(g+i)$ onto $X_{n-(g+i)}$, the variety $S^{(i)}$ is carried onto a variety we shall continue to denote by $S^{(i)}$, so that

$$S^{(i)}\subset X_{n-(g+i)},\qquad i=-1,\cdots,g-2,\cdots. \tag{3}$$

In particular, note the extreme cases: $S^{(-1)}=X_{n-g+1}=X_p$ since every divisor of degree $g-1$ is special and $S^{(g-1)}$ together with the higher $S^{(i)}$ are all empty.

We first note that set-theoretically,

$$\pi(S^{(i)})=U_{i+2},\qquad i=-1,\cdots,g-2. \tag{4}$$

This shows, incidentally, that if $i<j\leqq g-2$, then $S^{(i)}\neq S^{(j)}$. To prove it, using (1) and (2) above, we have

$$\mathfrak{b}^{g+i}+(n-g-i)p_0\in S^{(i)}\Longleftrightarrow \mathfrak{b}^{g+i}\text{ special}$$
$$\Longleftrightarrow |\mathfrak{k}-\mathfrak{b}|\text{ contains }\mathfrak{a}^{g-i-2}\text{ for some }\mathfrak{a}$$

$$\Longleftrightarrow \mathfrak{k}-\mathfrak{a}\sim\mathfrak{b} \Longleftrightarrow \mathfrak{b}-(g+i)p_0\sim\mathfrak{k}-\mathfrak{a}-(g+i)p_0$$

$$\Longleftrightarrow \mathrm{Cl}(\mathfrak{b}-(g+i)p_0) \text{ contains for some } \mathfrak{a} \text{ a divisor } \mathfrak{k}-\mathfrak{a}^{g-i-2}-(g+i)p_0$$

$$\Longleftrightarrow (\mathfrak{b}+(n-g-i)p_0)\in U_{i+2}.$$

Our main effort now goes into proving now the basic relation

$$\pi^{-1}(U_i)\cdot X_{p-i}=S^{(i-2)}+S^{(i-1)}, \qquad i=1,\cdots,g, \quad p=n-g+1. \tag{5}$$

From this our theorem follows easily. For writing (5) out for different i,

$$\begin{aligned}
&\pi^{-1}(U_1)\cdot X_{p-1}=X_p+S^{(0)} && \text{since } X_p=S^{(-1)},\\
&\pi^{-1}(U_2)\cdot X_{p-2}=S^{(0)}+S^{(1)},\cdots,\\
&\pi^{-1}(U_{g-1})\cdot X_{p-g+1}=S^{(g-3)}+S^{(g-2)},\\
&\pi^{-1}(U_g)\cdot X_{p-g}=S^{(g-2)} && \text{since } S^{(g-1)}=\phi,
\end{aligned}$$

so that alternately adding and subtracting, we get

$$X_p=\pi^{-1}(U_1)\cdot X_{p-1}-\pi^{-1}(U_2)\cdot X_{p-2}+\cdots+(-1)^{g-1}\pi^{-1}(U_g)\cdot X_{p-g}$$

which is the desired relation.

Proof of relation (5). We first show the relation is true set-theoretically. The right hand side is clearly contained in the left, since if we remember that $X^i=X_{n-i}$ by our conventions, we have using (3),

$$S^{(i-2)}\subset X^{g+i-2}\subset X^{g+i-1}, \qquad S^{(i-1)}\subset X^{g+i-1}=X^{n-p+i}=X_{p-i}.$$

Also, by (4) we have since $W_{i+1}\subset W_i$,

$$\pi(S^{(i-2)})=U_i, \qquad \pi(S^{(i-1)})=U_{i+1}\subset U_i.$$

Looking at the reverse inclusion, we have using (1) and (2),

$$\pi(\mathfrak{a}^{g+i-1}+(n-g-i+1)p_0)\in U_i \Longleftrightarrow \mathfrak{a}\sim\mathfrak{k}-\mathfrak{b}+p_0 \text{ for some } \mathfrak{b}^{g-i}$$
$$\Longleftrightarrow \mathfrak{a}-p_0 \text{ is special.}$$

There are two possibilities: either $\dim\mathfrak{a}=\dim(\mathfrak{a}-p_0)$ or else $\dim\mathfrak{a}=1+\dim(\mathfrak{a}-p_0)$. In the first case, p_0 is a fixed point of $|\mathfrak{a}|$, so $\mathfrak{a}=p_0+\mathfrak{a}^{g+i-2}$, where $\mathfrak{a}_0$ is special, so that $\mathfrak{a}_0+(n-g-i+2)p_0$ is in $S^{(i-2)}$. In the second case, since $\dim(\mathfrak{a}-p_0)>i-2$ (speciality), we deduce $\dim\mathfrak{a}>i-1$, so that $\mathfrak{a}$ is special, hence $\mathfrak{a}+(n-g-i+1)p_0$ is in $S^{(i-1)}$.

We have finally to show the relation (5) is true as an intersection formula, that is, that the coefficients of the right side are both one. Suppose then that

$$\pi^{-1}(U_i)\cdot X_{p-i}=aS^{(i-2)}+bS^{(i-1)}, \qquad a,b>0.$$

Let $\mathfrak{o}^{g-1}$ be a generic divisor of degree $g-1=n-p$. Then by Proposition 1, $X_{p-i}\cdot X[\mathfrak{o}]$ is defined and equals $X[\mathfrak{o}+(p-i)p_0]$. If now we can show that

(i) the cycle $Z = \pi^{-1}(U_i)\cdot X[\mathfrak{o} + (p-i)p_0]$ is defined, $i = 1,\cdots,g$, it will follow by the associativity formula that

$$Z = aS^{(i-2)}\cdot X[\mathfrak{o}] + bS^{(i-1)}\cdot X[\mathfrak{o}].$$

This, combined with

(ii) Z consists of points occurring all with multiplicity one,

(iii) $S^{(j)} \cap X[\mathfrak{o}]$ is not empty, $j = -1,\cdots,g-2$,

will then imply that both a and b are one, completing the proof of the theorem.

To prove statement (i), we have as before using (1) and (2),

$$\begin{aligned}\pi(\mathfrak{a}^i + \mathfrak{o} + (p-i)p_0) \in U_i &\Longleftrightarrow \mathfrak{a} + \mathfrak{o} \sim \mathfrak{k} - \mathfrak{b}^{g-i} + p_0 \text{ for some } \mathfrak{b}\\ &\Longleftrightarrow \mathfrak{a} + \mathfrak{b} \sim \mathfrak{k} + p_0 - \mathfrak{o}.\end{aligned}$$

Now $|\mathfrak{k} + p_0|$ has dimension $g-1$, so that since $\mathfrak{o}^{g-1}$ is generic,

$$\dim|\mathfrak{k} + p_0 - \mathfrak{o}| = 0$$

and the system contains a unique positive divisor of degree g. Thus $\mathfrak{a} + \mathfrak{b}$ is a well-determined divisor of degree g, which means that $\mathfrak{a}$ must be one of the (in general) ${}_gC_i$ divisors contained in it. In other words,

$$\pi^{-1}(U_i) \cap X[\mathfrak{o} + (p-1)p_0]$$

consists of a finite set of points.

Going on to statement (ii) now, apply to (i) the map π and use the projection formula, obtaining

$$\pi(Z) = U_i\cdot\pi(X[\mathfrak{o}^{n-p} + (p-i)p_0]) = U_i\cdot(W_{g-i})_x,$$

where $x = \pi(\mathfrak{o} + (n-g+1)p_0) = \pi(\mathfrak{o})$. It clearly is sufficient to show that $\pi(Z)$ has no multiple points, or by performing a translation by $-x$ on J and remembering $U_i = (W_i)_c$, that $W_{g-i}\cdot(W_i^-)_{c-x}$ has no multiple points. However, A. Weil has computed this zero-cycle for us [12, Prop. 17, p. 74], the result being $\sum(w_{\alpha_1\cdots\alpha_i})$, where the sum is taken over the ${}_gC_i$ combinations of indices $\alpha_1,\cdots,\alpha_g$ taken i at a time, the points

$$w_{\alpha_1\cdots\alpha_i} = \phi(q_{\alpha_1}) + \cdots + \phi(q_{\alpha_i})$$

and the q_{α_j} are defined by $c - x = \sum_1{}^g\phi(q_k)$; in these last two equations, ϕ is the canonical map of C into J, and the sums are taken in the sense of the group law on J. Our job is therefore to see that the $w_{\alpha_1\cdots\alpha_i}$ are all distinct.

The q_k are determined by the above according to the relation $\mathfrak{k} - \mathfrak{o} + p_0 \sim \sum q_k$, so we have to show that no two of the divisors of degree i contained in $(q_1 + \cdots + q_g)$ are linearly equivalent. The system $|\mathfrak{k} + p_0|$ has dimension $g-1$ and p_0 as fixed point. One divisor of this system is by the above $\mathfrak{o}+\sum q_k$; it is in fact a generic divisor (since $\mathfrak{o}$ is generic), and since p_0 is a fixed point of the system, say $p_0=q_g$. Then $\mathfrak{o}+(q_1+\cdots+q_{g-1})$ is a generic divisor of the canonical system $|\mathfrak{k}|$. But then the points $q_1,\cdots,q_{g-1}$ are independent generic points: in the non-hyperelliptic case because the canonical system has the independence property, while in the hyperelliptic case it is clear since a generic canonical divisor of $|\mathfrak{k}|$ is writable $\sum t_i+t_i'$, where t_i and t_i' are conjugates over a quadratic subfield of $k(C)$. There are thus three cases. Let $\mathfrak{a}^i$ and $\mathfrak{b}^i$ be two different divisors selected from $(q_1+\cdots+q_{g-1}+p_0)$. If both contain p_0 or if neither does, they cannot be linearly equivalent since, after subtracting the p_0 if necessary, two generic divisors of degree $\leqq g$ cannot be linearly equivalent, while if one contains p_0 but not the other, it is still impossible because a generic divisor of degree $i\leqq g$ has dimension zero and is therefore not linearly equivalent to another divisor of the same degree.

Finally to prove statement (iii), since the canonical system is of dimension $g-1$, we have (as in the preceding proof) a uniquely determined canonical divisor of the form $(q_1+\cdots+q_{g-1})+\mathfrak{o}^{g-1}$. Then clearly $\mathfrak{o}+(q_1+\cdots+q_{j+1})$ is a special divisor of degree $g+j$ (if $j=-1$, take just $\mathfrak{o}$), and so $S^{(j)}\cap X[\mathfrak{o}]$ cannot be empty because it contains

$$\mathfrak{o}+(q_1+\cdots+q_{j+1})+(n-g-j)p_0.$$

8. The Euler characteristic. Out of curiosity, and in order to sneak Newton into this paper, we compute the Euler characteristic of the vector bundle whose Chern classes we have just determined in Theorem 3.

The Chern classes of J—that is, the Chern classes of the tangent bundle to J—are trivial, since the tangent bundle is trivial: it is enough to show that the dual bundle of 1-forms is trivial, but this is evident because it has a basis at every point consisting of the g linearly independent invariant regular simple differentials on J. The Riemann-Roch-Hirzebruch formula [2] thus reduces to

$$\chi=\kappa_g(e^{\delta_1}+\cdots+e^{\delta_p}),$$

where the δ_i are defined formally, by the Corollary to Theorem 3, by

$$1-u_1x+u_2x^2-\cdots(-1)^g u_g=(1+\delta_1x)\cdots(1+\delta_gx),$$
$$\delta_i=0,\ i>g.$$

Expanding the exponential series and looking just at the term of weight g, we get

$$\chi=\kappa_g[(1/g!)(\delta_1{}^g+\cdots+\delta_g{}^g)].$$

Letting $s_k = \delta_1{}^k + \cdots \delta_g{}^k$, we now invoke, for $k = 1, \cdots, g$; [9],

Newton's identities: $s_k + u_1 s_{k-1} + \cdots + u_{k-1} s_1 = -k u_k$.

These give a system of linear equations for determining the s_k, whose solution for s_g is by Cramer's rule,

$$s_g = \begin{vmatrix} -g u_g & u_1 & u_2, \cdots, u_{g-1} \\ -(g-1) u_{g-1} & 1 & u_1, \cdots, u_{g-2} \\ \cdot & \cdot & \cdot \qquad \cdot \\ \cdot & \cdot & \cdot \qquad \cdot \\ -u_1 & \cdot & \cdot \qquad 1 \end{vmatrix} .$$

According now to intersection formulas of Matsusaka and Weil modulo numerical equivalence [7], $u_1{}^m \equiv m! u_m$, from which we deduce, if $\sum i_k = g$,

$$u_{i_1} u_{i_2} \cdots u_{i_r} \equiv (u_1{}^{i_1}/i_1!) \cdots (u_1{}^{i_r}/i_r!) \equiv g! u_g / i_1! \cdots i_r!.$$

All the terms in the above determinant, when it is expanded out, are indeed of weight g, and we get therefore

$$\chi = \kappa_g[(1/g!) s_g] = \begin{vmatrix} -g(1/g!) & 1 \ \tfrac{1}{2}! \cdots 1/(g-1)! \\ -(g-1)/(g-1)! & 1 \ 1 \cdots 1/(g-2)! \\ \cdot & \\ \cdot & \\ -1 & \cdot \cdot \cdot \cdot \cdot \quad 1 \end{vmatrix} .$$

Thus $\chi = 0$, since the first and last columns differ by a sign.

9. Some relations in $A(J)$. Quite generally, if $(P(E), X, \pi)$ is a projective bundle derived from a vector bundle E of rank p over a base space X of dimension g and $\xi \in A_1(P(E))$ is the associated divisor class, we can deduce trivially from the Chern relation

$$\xi^p + c_1{}^* \xi^{p-1} + c_2{}^* \xi^{p-2} + \cdots + c_p{}^* = 0$$

some relations in $A(X)$. Namely, multiply the relation through by ξ^i, $i = 0, \cdots, g-1$, project onto X and use the projection formula; this gives

$$\pi(\xi^{p+i}) + c_1 \pi(\xi^{p+i-1}) + \cdots + c_p \pi(\xi^i) = 0 \qquad i = 0, \cdots, g-1,$$

a set of relations which may be summarized as

$$(1 + c_1 + c_2 + \cdots + c_p)(1 + \pi(\xi^p) + \pi(\xi^{p+1}) + \cdots + \pi(\xi^{p+g-1})) = 1,$$

in view of the fact that $\pi(\xi^{p-1}) = 1$, $\pi(\xi^j) = 0$ if $j < p-1$.

Applying this to our situation, we have $\pi(\xi^{p+i}) = w_{i+1}$, and so

$$(1 - u_1 + u_2 - \cdots + (-1)^g u_g)(1 + w_1 + w_2 + \cdots + w_g) = 1;$$

written in terms of the cycles, this becomes

THEOREM 4. *If w_i is the rational equivalence class of W_i (in Weil's notation W_{g-i}) on J and u_i the class of $W_i^* = (W_i^-)_c$, then*

$$\begin{aligned} &w_1 - u_1 = 0,\\ &w_2 - u_1 w_1 + u_2 = 0, \cdots,\\ &w_g - u_1 w_{g-1} + \cdots + (-1)^g u_g = 0. \end{aligned}$$

These express therefore the u_i in terms of the w_i. The nature of the relations suggest that if one applies the map $\sigma\colon x \to -x + c$ to J, the resulting projective bundle $(C(n), J, \sigma\pi)$ whose Chern classes are $(-1)^i w_i$—or rather, prehaps its dual—should be in some sense the "opposite" bundle to $(C(n), J, \pi)$.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

REFERENCES.

[1] A. Andreotti, "On a Theorem of Torelli," *American Journal of Mathematics*, vol. 80 (1958), pp. 801-828.

[2] A. Borel and J. P. Serre, "Le Theoreme de Riemann-Roch," *Bulletin de la Société Mathématique de France*, vol. 86 (1958), pp. 97-136.

[3] W.-L. Chow, "The Jacobian variety of an algebraic curve," *American Journal of Mathematics*, vol. 76 (1954), pp. 453-476.

[4] ———, "Remarks on my paper, 'The Jacobian variety of an algebraic curve,'" *ibid.*, vol. 80 (1958), pp. 238-240.

[5] A. Grothendieck, "La théorie des classes de Chern," *Bulletin de la Société Mathématique de France*, vol. 86 (1958), pp. 137-154.

[6] ———, "Sur quelques points d'algèbre homologique," *Tôhoku Mathematical Journal*, 2nd series, vol. 9 (1957), pp. 119-221.

[7] T. Matsusaka, "On a characterization of a Jacobian variety," *Memoirs of the College of Science, University of Kyoto*, Series A, vol. 32, Math. no. 1 (1959), pp. 1-19.

[8] A. Mattuck, "Picard bundles," to appear.

[9] I. Newton, *Arithmetica Universalis*, 1707.

[10] G. Washnitzer, "The characteristic classes of an algebraic fiber bundle, I," *Proceedings of the National Academy of Sciences*, vol. 42 (1956), pp. 433-436.

[11] A. Weil, *Fiber spaces in Algebraic Geometry*, mimeographed notes, University of Chicago, 1952.

[12] ———, *Variétés Abéliennes et Courbes Algébriques*, Paris, 1948.

CORRECTION TO "APPLICATIONS OF THE THEORY OF MORSE TO SYMMETRIC SPACES" (This Journal, vol. 80 (1958), pp. 964-1029).*

By RAOUL BOTT and HANS SAMELSON.

It has been pointed out to us by H. Seifert that our characterization of simplices "hanging over critical points" in the paper cited above (conditions (a) (b) (c) on p. 978) is insufficient and that therefore our description of the theory of Morse in Proposition 8. 3, p. 978, is incorrect as stated. If the space Ω were a manifold, one would only have to add the requirement that the singular simplices in question be differentiable and non-degenerate (have non-singular differential, at least at the barycenter). But in a function space the description of the associated simplices is more complicated. One of Morse's procedures (cf. [16, pp. 38, 56, 58; 17, pp. 52, 81]) is to introduce a set of cross manifolds Q_k (including the end-manifold) along the geodesic segment s, and with their help to imbed the point s of Ω into a manifold $P_s = \prod_k Q_k$ of geodesic polygons, contained in Ω. The function $L \mid P_s$ is C^∞ and has a non-degenerate singularity of index λ_s at s. The main fact is now that any singular simplex associated to s in P_s also serves as associated simplex in Ω. With this in mind we shall prove below that the singular simplex (σ_s, ϕ_s) of p. 984, l. 27 is indeed associated to s. (This is where we had used our incorrect characterization.) The remainder of the proof on pp. 984, 985 is unchanged. Proposition 10. 2(d), p. 981, and its proof in Section 11, pp. 983, 984, become unnecessary.

We may and shall assume that among the Q_k there is one at each exceptional point $s(t_i)$ and one at some point $s(\bar{t}_i)$ with $\bar{t}_i$ in (t_i, t_{i+1}) for $i = 1, \cdots, n$; further each cross manifold contains locally the orbit of the point to which it is attached.

The map $f_s\colon \Gamma_s \to \Omega$, restricted to a small neighborhood of ω_s, factors then through a C^∞-map h_s into P_s.

LEMMA (a). *h_s is non-degenerate at ω_s.*

Proof. Let X be a non-zero vector of Γ_s at ω_s; let Y be a vector of W_s at $(e, \cdots, e)$ with $\dot{\psi}_s(Y) = X$. We write $Y = (Y_1, \cdots, Y_n)$, with Y_j a vector of K_j. Let Q be a cross manifold, attached to some $\bar{t}_i$. The image of X under the composition of h_s, projection of P_s onto its factor Q, and inclusion of Q in M is easily found to be $(\tilde{Y}_1 + \cdots + \tilde{Y}_i)(s(\bar{t}_i))$ (cf. def. 1. 6 for $\tilde{Y}$).

---

* Received December 20, 1960.

If i is the smallest value for which Y_i is not tangent to the subgroup K_s of K_i (this exists since $K \neq 0$), the vector so obtained is not zero, since $\bar{t}_i$ is not exceptional, and Lemma (a) is proved.

Next we consider a local lemma. Let f be a C^∞-function on a neighborhood U of a point p in a manifold of dimension m, with p as only critical point, non-degenerate, of index λ. Write A for $\{x \in U : f(x) \leqq f(p)\}$, A^- for $\{x \in U : f(x) < f(p)\}$, A_0 for $\{x \in U : f(x) = f(p)\}$.

Let $\mu \colon \sigma \rightarrow U$ be a C^∞-singular simplex of dimension λ such that

(i) $\mu^{-1}(p)$ consists of just the barycenter b of σ,

(ii) $f \circ \mu$ is constant, i. e., $\mu(\sigma) \subset A_0$,

(iii) the differential of μ is non-singular at b.

LEMMA (b). *Under the above hypothesis, μ represents a generator of $H_\lambda(A, A - \{p\})$, for any coefficient group. Further, if $\mu' \colon \sigma \rightarrow U$ is a singular simplex sufficiently close to μ, with $\mu'(\sigma) \subset A^- \cup \{p\}$, then μ' is a generator of $H_\lambda(A^- \cup \{p\}, A^-)$, again for any coefficient group, i. e. it serves as associated simplex for the critical point p.*

Proof. We may assume (by [16]) that $U =$ Euclidean space E^m, that p is the origin and that f has the form $-x_1^2 - \cdots - x_\lambda^2 + x_{\lambda+1}^2 + \cdots + x_m^2$. Both pairs $(A, A - \{p\})$ and $(A^- \cup \{p\}, A^-)$ have as deformation retract the pair $(E^\lambda, E^\lambda - \{p\})$, where E^λ is th subspace of E^m spanned by the first λ axes; the retraction map is identical with the projection θ along the orthogonal complement of E^λ. Because of (iii) the "light cone" A_0 contains linear subspaces of dimension λ; any such space maps in non-degenerate fashion under θ. The differential of $\theta \circ \mu$ is therefore non-degenerate at b, and the lemma follows by standard arguments. Incidentally, λ is necessarily $\leqq m/2$.

We come now to the proof that the simplex (σ_s, ϕ_s) of no. 12, p. 984, is associated to s. The simplex $h_s \circ \rho_s \colon \sigma_s \rightarrow P_s$ (defined if $\rho_s(\sigma_s)$ is small enough) satisfies the hypotheses of Lemma (b); (i) is clear, (ii) follows from the second sentence on p. 981, and (iii) is implied by Lemma (a). The standard retraction of a neighborhood of s (in Ω) into P_s sends the singular simplex ϕ_s into a singular simplex ϕ_s' with $\phi_s'(\sigma_s) \subset P_s$. Since the L-value does not increase under the retraction, Lemma (b) applies, so that ϕ_s', being close to $h_s \circ \rho_s$ for small u, is associated to s in P_s; but then ϕ_s is associated to s in Ω. Q. E. D.

HARVARD UNIVERSITY,
INSTITUTE FOR ADVANCED STUDY,
AND STANFORD UNIVERSITY.

UNIVE

MAPPINGS OF PARTIALLY ANALYTIC SPACES.*

By Errett Bishop.

---

1. Introduction. We study a mapping f of a partially analytic space K into n-dimensional complex affine space C^n. A partially analytic space K is a Hausdorff topological space which is a countable union of conditionally compact open sets, which is locally connected, and which is endowed, at least partially, with an analytic structure. This means that a countable family $\{M_\alpha\}$ of subsets of K is given, each with the structure of a complex analytic manifold. An algebra $\mathfrak{A}$ of continuous functions on K, called the analytic functions on K, is also given, with the property that each function in $\mathfrak{A}$ is analytic on each M_α. The algebra $\mathfrak{A}$ is closed in the topology of uniform convergence on compact subsets of K. The coordinates of the mapping f are required to lie in $\mathfrak{A}$. The purpose of this paper is to show that for certain spaces K the mapping f can be chosen to have certain properties. For instance, sufficient conditions are given for there to exist an f which is proper, or which separates points, or which has a certain rank at certain points. Since the complex spaces of Cartan [4] or Behnke and Stein [2] can be thought of as partially analytic spaces, these results apply to complex spaces.[1]

Theorem 1 is concerned with the dimensions of the level sets of the mapping f. The statement of Theorem 1 is somewhat complicated; a special case reads as follows. If the level sets of $\mathfrak{A}$ intersect each M_α in a countable set, then f can be chosen so that the level sets of f intersect each M_α in a set of (complex) dimension at most $\max\{d_\alpha - n, 0\}$, where $d_\alpha = \dim M_\alpha$. Theorem 1 is closely related to a theorem of Grauert ([6], Satz 12), but the proof given here differs from Grauert's proof and a more general theorem is obtained.

The next part of the paper is concerned with analytic polyhedra. With f as above, write

$$P_0 = \{p : p \in \cup M_\alpha . \, |f_i(p)| < 1, 1 \leqq i \leqq n\}.$$

An analytic polyhedron P in K defined by f is a subset of P_0 which is both open and closed in P_0 and whose closure is a compact subset of $\cup M_\alpha$.

---

* Received June 1, 1960.

[1] See in this regard however footnote 3.

Theorem 3 states that if S is a compact subset of P then there exists an analytic mapping g of K into C^d which defines an analytic polyhedron Q with $S \subset Q \subset P$, where d is the maximum of the dimensions of the M_α (which is assumed to be finite). Theorem 3 (in a more general form) is basic to the theorems which follow. To prove Theorem 3, one first modifies the mapping $f = (f_1, \cdots, f_n)$ slightly so that for each α the sets of simultaneous constancy of the functions $f_2/f_1, \cdots, f_n/f_1$ on

$$H_\alpha = P \cap \{p : f(p) \neq 0\} \cap M_\alpha$$

have the same dimension at each point of H_α as the sets of simultaneous constancy of $\mathfrak{A}$. That this can be done follows from Theorem 1 if $n > d$, and if $n \leqq d$ there is nothing to prove. This modification of f having been made, choose the constant $r > 1$ such that $|f_i(p)| < r^{-1}$ for all p in S and $1 \leqq i \leqq n$, and write

$$g_i = (rf_i)^N - (rf_1)^N, \qquad 2 \leqq i \leqq n.$$

Then if N is sufficiently large the mapping $g = (g_2, \cdots, g_n)$ of K into C^{n-1} defines an analytic polyhedron P' with $S \subset P' \subset P$. After $n - d$ such constructions one obtains the analytic ployhedron Q of Theorem 3.

Next it is assumed that K is weakly holomorphically convex, which means that $K = \cup M_\alpha$ and that for each compact $S \subset K$ each component of the set

$$\tilde{S} = \{p : p \in K, |f(p)| \leqq \max_{q \in S} |f(q)| \text{ for all } f \text{ in } \mathfrak{A}\}$$

is compact. Since weak holomorphic convexity implies that K is the union of an increasing sequence of analytic polyhedra, one is able to apply Theorem 3 to show (Theorem 4) that K admits an almost proper analytic map f into C^d, where d is the maximum of the dimensions of the M_α and where almost proper means that each component of the inverse image of a compact set is compact.

There follows a section of the paper devoted to the study of certain special analytic polyhedra (Theorem 5). As a result of this study we obtain some integral formulas (Theorems 6 and 7) which are an attempt to generalize the usual one dimensional planar formula to several dimensions and to manifolds. These formulas recall the several dimensional integral formulas of Weil [13] and Bergmann [3], although they seem to be fundamentally different from those formulas.

Next we return to the study of mappings and show (Theorem 8) that if K is weakly holomorphically convex, if $\mathfrak{A}$ separates points of K, and if certain other minor conditions are satisfied, there exists a proper mapping of K into C^{d+1}, with d as above, where proper means that the inverse images of compact sets are compact. The proof of this theorem goes as follows. Let f be an almost proper mapping of K into C^d. Let $\{S_k\}$ be an increasing sequence of compact sets the union of whose interiors is K. Let

$$J_k = \{z : z = (z_1, \cdots, z_d) \in C^d, |z_i| \leqq k \text{ for } 1 \leqq i \leqq d\}.$$

For each positive integer k let H_k be the union of those components of $f^{-1}(J_k)$ which intersect S_k. Let G_k be the set $[f^{-1}(J_k) \cap H_{k+1}] - H_k$. The sets G_k and H_k are disjoint compact sets. If $\mathfrak{A}_k$ denotes the set of all uniform limits on $G_k \cup H_k$ of functions in $\mathfrak{A}$, it can be shown that the maximal ideal space of the Banach algebra $\mathfrak{A}_k$ is just the set $G_k \cup H_k$. It follows from the general theory of Banach algebras that there exists ω_k in $\mathfrak{A}$ arbitrarily large on G_k and arbitrarily small on H_k. Since $\{H_k\}$ is an increasing sequence of compact sets the union of whose interiors is K, it follows that the functions ω_k can be chosen so that the series $\sum_{k=1}^{\infty} \omega_k$ converges uniformly on compact subsets of K to a function f_{d+1} in $\mathfrak{A}$ with $|f_{d+1}(p)| > k$ for all p in G_k and all k. To see that the mapping $f \times f_{d+1}$ of K into C^{d+1} is proper, write

$$F_k = \{p : p \in K, |f_i(p)| \leqq k \text{ for } 1 \leqq i \leqq d+1\},$$

and consider p in F_k. Let j be the smallest integer not less than k such that $p \in H_j$. If $j > k$ then $p \in G_{j-1}$. Therefore $k \geqq |f_{d+1}(p)| > j-1$. This contradiction shows that $j = k$, so that $p \in H_k$. Thus $F_k \subset H_k$, so that F_k is compact and the mapping $f \times f_{d+1}$ is proper.

It is now relatively simple (Theorem 9) in case K, for instance, is a Stein manifold to choose functions $f_{n+2}, \cdots, f_{2n+1}$ in $\mathfrak{A}$ such that $(f_1, \cdots, f_{2n})$ has rank n at each point of K and $(f_1, \cdots, f_{2n+1})$ distinguishes points of K. This is done by choosing the functions successively to decrease the dimensions of certains singular sets associated with the mapping.

This last result is a special case of as yet unpublished results[2] on the problem by R. Narasimhan, who used other methods. The first result of this type is due to Remmert [8].

If one looks at the proofs more closely, it can be seen that all of the mappings considered are dense in the topology of uniform convergence on compact subsets of K.

It is intended to devote a subsequent paper to applications of the results given here.

---

[2] Since this was written Narasimhan's paper has appeared in *American Journal of Mathematics*, vol. 82 (1961), pp. 917-934.

2. Dimensions of level sets of mappings. Rather then begin by considering what is known in the literature as analytic space we introduce a notion which is somewhat more general and which is sufficient for the purposes of this section.

Definition 1. A *partially analytic space* K consists of a Hausdorff space K, a countable family $\{M_\alpha\}$ of subsets of K, each of which is a (complex) analytic manifold, and a set $\mathfrak{A}$ of continuous (complex-valued) functions on K. The relative topologies of the subsets M_α are the same as the topologies which they possess as analytic manifolds. The space K is a countable union of open sets whose closures are compact, and each component of an open set in K is open. Each function in $\mathfrak{A}$ is analytic on each M_α. $\mathfrak{A}$ is closed in the topology of uniform convergence on compact subsets of K. Also $\mathfrak{A}$ is an algebra in the sense that sums, products, and complex multiples of elements in $\mathfrak{A}$ are in $\mathfrak{A}$.

In the above definition and in the sequel an analytic manifold will be understood to be connected and coverable by a countable number of coordinate neighborhoods. Thus each M_α has a (complex) dimension d_α, which is the same as the dimension of M_α at each of its points.

As an abbreviation, we speak of a partially analytic space K, the rest of the structure—the manifolds M_α, called the structure manifolds of K, and the algebra $\mathfrak{A}$, called the set of analytic functions on K—being understood.

The set of continuous complex-valued functions on K is written $C(K)$, and the subset of $C(K)$ consisting of those functions analytic on each M_α is written $A(K)$. The set of all analytic functions on an analytic manifold M is written $A(M)$. The topology of uniform convergence on compact subsets of K is easily seen to be a metrizable topology for $C(K)$. To see this, let $\{F_n\}$ be a sequence of compact sets whose interiors cover K, and let

$$\| f \|_n = \sup\{ | f(p) | : p \in F_n\}$$

for each f in $C(K)$. Let

$$\rho(f, g) = \sum_{n=1}^{\infty} 2^{-n} \| f - g \|_n (1 + \| f - g \|_n)^{-1}$$

for all f and g in $C(K)$. Then ρ is a metric for $C(K)$ and $C(K)$ is complete in the metric ρ. As a closed subset of $C(K)$, $\mathfrak{A}$ is also a complete metric space with metric ρ.

We now recall some standard material from the theory of several complex variables which will be of use later. See in this connection the notes [4], [5], and [10], and the paper [12]. A set A in an analytic manifold M is *analytic* if to each point p of M there exists a neighborhood U of p and a finite set of analytic functions on U such that $A \cap U$ is the set of common zeros in U of the functions. A set A is *locally analytic* in M if to each p in A there exists a neighborhood U of p and a finite set of analytic functions on U such that $A \cap U$ is the set of common zeros in U of the functions. A locally analytic set is analytic if and only if it is closed. A point p of a locally analytic set A in a manifold M is called *regular* if there exists a coordinate neighborhood U of p and coordinate functions $f_1, \cdots, f_n$ on U such that

$$A \cap U = \{q : f_i(q) = 0, 1 \leqq i \leqq k\}$$

for some positive integer k. The set A_R of regular points of a locally analytic set A is a locally analytic set which is open and dense in A; if $A = A_R$, then A is called a regular locally analytic set. A connected regular locally analytic set is called a submanifold of M. Then A_R has a countable number of components, each open in A, each of which is a submanifold of M and each of which inherits from M in a natural way the structure of an analytic manifold. The (complex) dimension of A, which equals one-half of the topological dimension of A, is the maximum of the dimensions of the components of A_R. If p is a point in A, the local dimension of A at p is the minimum of the dimensions of the locally analytic sets $A \cap U$, where the sets U are neighborhoods of p. The dimension of A is the maximum of the local dimensions of its points. The set $A_S = A - A_R$ is a locally analytic set whose dimension is strictly less than that of A; it is an analytic set if A is an analytic set. This gives rise to a sequence

$$A = A^0 \supset A^1 \supset \cdots \supset A^k$$

of locally analytic sets, each a closed subset of the preceding, such that $A^i = (A^{i-1})_S$ for $1 \leqq i \leqq k$ and such that A^k is empty. Thus A is the union of the disjoint regular locally analytic sets $(A^i)_R$, $0 \leqq i \leqq k-1$. It follows that A is a countable union of disjoint submanifolds $\{M_\alpha\}$ of M. Thus A can be made into a partially analytic space by considering it as a Hausdorff space with structure manifolds $\{M_\alpha\}$ and by choosing $\mathfrak{A}$ for instance to be the set of holomorphic functions on A. It is also clear that a complex space (a concept which we do not use here: see [2] or [4]), which locally has the structure of an analytic set in an analytic manifold, can be thought of as a partially analytic space.[3]

---

[3] The referee has pointed out that this fact, while true, is not trivial if $\mathfrak{A}$ consists of all functions on an analytic space K which are analytic in the narrow sense, that is,

Definition 2. A set $f_1, \cdots, f_d$ of analytic functions of a d-dimensional analytic manifold M will be called a *coordinate set* of functions at a point p in M if there exists a neighborhood U of p and a constant $r > 0$ such that

$$f \colon q \to (f_1(q), \cdots, f_d(q))$$

maps U homeomorphically onto the set

$$E = \{z = (z_1, \cdots, z_d) : |z_i - f_i(p)| < r, 1 \leqq i \leqq d\}$$

in d-dimensional complex affine space C^d. The set U will then be called a *coordinate neighborhood* of p for the functions $f_1, \cdots, f_d$.

LEMMA 1. *Let K be a partially analytic space with a single structure manifold M. Let m be a positive integer not larger than the dimension d of M. Let $f_1, \cdots, f_d$ in $A(M)$ be a coordinate set of functions at a point p of M, and let U be an associated coordinate neighborhood,*

$$f(U) = \{z = (z_1, \cdots, z_d) : |z_i - f_i(p)| < r, 1 \leqq i \leqq d\}.$$

Let f_m be in $\mathfrak{A}$ and h in $A(M)$. Then the set G of functions g in $\mathfrak{A}$ such that the level sets V (sets of simultaneous constancy) of the functions $f_1, \cdots, f_{m-1}, g + h$ on U are all of dimension $d - m$ or less is dense in $\mathfrak{A}$ and is a countable intersection of open subsets of $\mathfrak{A}$.

Proof. Let g_0 be any element of $\mathfrak{A}$ and ϵ a positive number. Let f_m assume the value b at some point in U. Define

$$g = g_0 + \sum_{j=1}^{d+1} \alpha_j (f_m - b)^j - \sum_{j=1}^{d+1} \alpha_j (-b)^j,$$

where the α_j are constants to be chosen. Thus $g \in \mathfrak{A}$ and $\rho(g, g_0) < \epsilon$ if the α_j are sufficiently small. Choose the α_j to be that small and in addition to have the property that the functions

$$(*) \qquad i!\alpha_i + \partial^i (g_0 + h) / \partial (f_m)^i, \qquad 1 \leqq i \leqq d + 1,$$

have no common zero in U. This is possible because the range of the mapping

$$\sigma \colon p \to (c_1, \cdots, c_{d+1}), c_i = \left.(i!)^{-1} \partial^i (g_0 + h) / (\partial f_m)^i \right]_p$$

of U into C^{d+1} has topological dimension at most $2d$ and therefore contains

---

which arise from functions analytic in open subsets of the analytic manifolds in which K is considered as locally imbedded. The difficulty in this case is to show that $\mathfrak{A}$ is closed in $C(K)$. This was proved by Grauert and Remmert in *Mathematische Annalen*, vol. 136 (1958), pp. 245-318.

no neighborhood of the origin. To see that g is in G, it is enough to show that $g + h$ is not constant on each of the coordinate planes

$$L = \{p\colon p \in U, f_i(p) = c_i, 1 \leqq i \leqq m - 1\},$$

since the sets V are then proper analytic subsets of such planes L and therefore have dimensions less than the dimensions $d - (m - 1)$ of the planes. Assume therefore that $g + h$ is constant on some plane L. Thus

$$\partial^i (g + h)/(\partial f_m)^i = \partial^i (g_0 + h)/\partial (f_m)^i + \sum_{j=1}^{d+1} \alpha_j (j!/(j - i)!)(f_m - b)^{j-i}$$

vanishes everywhere on L. If p_0 denotes a point of L for which $f_m(p_0) = b$, it follows that the functions (*) have a common zero at p_0. This contradiction to the choice of the constants α_j means $g \in G$. Since g_0 and ϵ were arbitrary, G is dense in $\mathfrak{A}$. To finish the proof of the lemma, define F_k, for each positive integer k, to consist of all g in $\mathfrak{A}$ such that there exists a coordinate plane L with $|c_i| \leqq r - k^{-1}$ for $1 \leqq i \leqq m - 1$ on which $g + h$ is constant. Clearly F_k is closed in $\mathfrak{A}$ and $\cup F_k = - G$. Thus $G = \cap (\mathfrak{A} - F_k)$. This completes the proof of the lemma.

Definition 3. If M is an analytic manifold, a subset S of $A(M)$ is said to have *dimension* m over a subset T of $A(M)$ at a point p of M, if the level set of T containing p includes the level set of S containing p and if the difference in the local dimensions at p of these two level sets is m. The set S is said to have dimension m_0 over T on M if each level set of S on M is contained in a level set of T on M and if m_0 is the maximum of m for p in M. If T is void, then one speaks simply of the dimension m of S at a point p or of the dimension m_0 of S on M. The *rank* of S at p is the rank at p of the Jacobian matrix of S with respect to some coordinate set of functions at p.

LEMMA 2. *Let K be a partially analytic space with a single structure manifold M of dimension d. Let B be a subset of $A(M)$ and h an element of $A(M)$. Let P consist of all points p in M such that the dimension of $\mathfrak{A} \cup B \cup \{h\}$ over B at p is at least* 1. *Let G be the set of all g in $\mathfrak{A}$ such that the dimension of $B \cup \{g + h\}$ over B at p is at least* 1 *for all p in P. Then $\mathfrak{A} - G$ is of the first category in $\mathfrak{A}$.*

Proof. The proof proceeds by induction on d. The lemma is clearly true if $d = 0$, since in that case the set P is void. Assume therefore that the lemma is true for all values of d less than the given value. At each point p in M let J_p be the (possibly infinite) Jacobian matrix of the functions in B with respect to a set of coordinates at p, and let J_p have rank m_p. Let m be the maximum of the m_p. Choose p_0 with $m_{p_0} = m$, and let $f_1, \cdots, f_m$ be elements of B whose Jacobian matrix at p_0 has rank m. Let V be the set of points in M where the Jacobian matrix of these functions has rank m, i.e., where these functions are part of a coordinate set of functions. Thus V is open in M.

The level sets of B have dimension $d - m$ at each point of V. Either the level sets of $\mathfrak{A} \cup B$ have dimension $d - m$ at each point of V (case I) or there exists g_0 in $\mathfrak{A}$ such that the Jacobian matrix of $f_1, \cdots, f_m, g_0$ has rank $m + 1$ at some point of V (case 1). In case 1, let W be the set of all points in M where the Jacobian matrix of $f_1, \cdots, f_m, g_0$ has rank $m + 1$. In case I, either the Jacobian matrix of $f_1, \cdots, f_m, h$ has rank m at every point of V (case 3) or has rank $m + 1$ at some point of V (case 2). In case 3 define $W = V$. In case 2 let W consist of those points of M at which the Jacobian matrix of $f_1, \cdots, f_m, h$ has rank $m + 1$. Thus we see that in all three cases W is a non-void open subset of M and $M - W$ is an analytic subset of M. Thus $M - W$ is the union of a countable family $\{M_\alpha\}$ of disjoint submanifolds of M. The dimension d_α of M_α is less than d. Let the partially analytic space K_α consist of the Hausdorff space K with the single structure manifold M_α and with the set of analytic functions $\mathfrak{A}$. Let P_α consist of all points p in M_α such that $\mathfrak{A} \cup B \cup \{h\}$ has dimension at least 1 over B at the point p on the manifold M_α. Since $d_\alpha < d$, it follows from the induction hypothesis that the set G_α of all g in $\mathfrak{A}$ such that $B \cup \{h + g\}$ has dimension at least 1 over B on the manifold M_α at all points of P_α has the property that $\mathfrak{A} - G_\alpha$ is of the first category in $\mathfrak{A}$.

Consider now case 1. For each point p in W, let U_p be a coordinate neighborhood of p for some coordinate set of functions containing the functions $f_1, \cdots, f_m, g_0$. Since the topology of M has a countable base, a countable family $\{U_j\}$ of the U_p covers M. From Lemma 1 it follows that $\mathfrak{A} - G_j$ is of first category in $\mathfrak{A}$, where G_j consists of all g in $\mathfrak{A}$ such that the level sets of $f_1, \cdots, f_m, g + h$ on U_j have dimension at most $d - m - 1$. Define

$$H = \bigcup_\alpha(\mathfrak{A} - G_\alpha) \cup \{\bigcup_j(\mathfrak{A} - G_j)\}.$$

In cases 2 and 3, define

$$H = \bigcup_\alpha(\mathfrak{A} - G_j).$$

Thus, in any case, H is of first category in $\mathfrak{A}$. We shall complete the proof by showing that $\mathfrak{A} - G \subset H$. To this end, consider g in $\mathfrak{A} - G$. Thus there exists p in P such that the dimension of $B \cup \{g + h\}$ at p equals the dimension of B at p. Let D, E, and F respectively be the level sets of B, of

$B \cup \{g+h\}$, and of $\mathfrak{A} \cup B \cup \{h\}$ which contain p. Let their respective dimensions at p be λ, μ, and ν. Thus $\lambda = \mu$. Since $p \in P$, we have $\nu < \lambda$. Let O_1 be a neighborhood of p such that $D \cap O_1$, $E \cap O_1$, and $F \cap O_1$ have dimensions λ, μ, and ν respectively. Since the level set $F \cap O_1$ of $\mathfrak{A} \cup B \cup \{h\}$ on O_1 which contains p has dimension ν, there exists a neighborhood $O \subset O_1$ of p such that every level set of $\mathfrak{A} \cup B \cup \{h\}$ on O has dimension at most ν (see [5], Exp. XIV). Now for each α the set $E \cap O \cap M_\alpha$ is a countable union of compact sets; so is the set $E \cap O \cap W$. Also, $E \cap O$ is the union of $E \cap O \cap W$ and the sets $E \cap O \cap M_\alpha$. By a standard theorem of dimension theory (see [7], p. 30), it follows that $\lambda = \dim(E \cap O)$ is the maximum of the dimensions of $E \cap O \cap W$ and the sets $E \cap O \cap M_\alpha$. Thus

$$\dim(E \cap O \cap Q) = \lambda,$$

where Q is either W or one of the sets M_α. Thus there exists a point p_0 in $E \cap O \cap Q$ such that the dimension of $E \cap Q$ at p_0 is λ. By the choice of O, the dimension at p_0 of the level set F_0 of $\mathfrak{A} \cap B \cap \{h\}$ containing p_0 is at most ν. Also, the dimension of the level set $D \cap Q$ of B at p_0 on Q is at least λ, since it contains the set $E \cap O \cap Q$ which has dimension λ at p_0; on the other hand, the dimension of $D \cap Q$ at p_0 is at most $\mu = \lambda$, and therefore this dimension equals λ.

Consider first the case in which $Q = M_\alpha$ for some α. Since $\nu < \lambda$ the dimension of $F_0 \cap M_\alpha$ at p_0 is less than the dimension of $D \cap Q = D \cap M_\alpha$ at p_0; therefore $p_0 \in P_\alpha$. Also the dimension of $D \cap M_\alpha$ at p_0 is λ and the dimension of $E \cap M_\alpha$ at p_0 is λ. By the definition of G_α, it follows that $g \in \mathfrak{A} - G_\alpha$. Thus $g \in H$.

It remains to consider the case $Q = W$ and to show that $g \in H$ in this case also. To do this, cases 1, 2, and 3 must be considered separately. Consider first case 1. Let U_j be one of the sets of the family $\{U_j\}$ which contains p_0. By the choice of $f_1, \cdots, f_m$ any function f in B must be constant on each component of each level set of these functions on W: otherwise, there would exist f in B such that the Jacobian of $f_1, \cdots, f_m, f$ with respect to a coordinate set of functions would be of rank $m+1$ at some point of W. Thus the dimension λ at p_0 of the level set $D \cap Q = D \cap W$ of B equals $d - m$. Since also λ is the dimension of the level set $E \cap W = E \cap Q$ of $B \cup \{g+h\}$ at p_0, it follows that $g \in \mathfrak{A} - G_j$. Thus $g \in H$.

Next consider case 2. Since the function g in $\mathfrak{A}$ is locally constant on the level sets in W of the coordinate functions $f_1, \cdots, f_m$, the level sets of $f_1, \cdots, f_m$, $g+h$ on W are locally the same as those of the functions

$f_1, \cdots, f_m$, h and therefore have dimension $d - m - 1$. Thus the dimensions at p_0 of the level sets of B and $B \cup \{g + h\}$ are $d - m$ and $d - m - 1$ respectively. This contradicts the fact, derived above, that both these dimensions are λ. Thus case 2 does not arise.

Next consider case 3. In this case it is clear that locally the level sets of B, $B \cup \{g + h\}$, and $\mathfrak{A} \cup B \cup \{h\}$ are the same as the level sets of $f_1, \cdots, f_m$. This contradicts the fact that the level sets of B and $\mathfrak{A} \cup B \cup \{h\}$ containing p_0 have respective dimensions λ and $\nu < \lambda$ at p_0. Thus case 3 also does not arise. This completes the proof of Lemma 2.

Definition 4 (by induction). Let X be the Cartesian product of complete metric spaces $X_1, \cdots, X_n$. If $n = 1$, then $F \subset X$ is said to be of *third category* if it is of first category. If $n > 1$, then F is said to be of *third category* if the set of all points p in $X_1 \times \cdots \times X_{n-1}$ for which the set of points q in X_n such that $(p, q) \in X$ is not of first category is of third category.

It is clear that a countable union of sets of third category is of third category, and that the complement of a set of third category is dense.

THEOREM 1. *Let K be a partially analytic space. For each α, let B_α be a subset of $A(M_\alpha)$ and let $h^1{}_\alpha, \cdots, h^k{}_\alpha$ be elements of $A(M_\alpha)$, where k is a fixed positive integer. Let $P^i{}_\alpha$, $1 \leqq i \leqq k$, consist of all p in M_α such that the dimension on the manifold M_α of $\mathfrak{A} \cup B_\alpha \cup \{h^1{}_\alpha, \cdots, h^k{}_\alpha\}$ over B_α at p is at least i. Let G be the set of all $g = (g_1, \cdots, g_k)$ in ${}^k\mathfrak{A}$ such that for each α, each i, and each p in $P^i{}_\alpha$ we have*

(*) *The dimension on the manifold M_α at p of*

$$B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_k + h^k{}_\alpha\}$$

over B_α is at least i.

Then ${}^k\mathfrak{A} - G$ is of third category in the k-fold cartesian product ${}^k\mathfrak{A}$ of $\mathfrak{A}$ with itself.

Proof. We show by induction on k that the theorem is true for all positive integers k. We assume that the theorem is true for all values of k smaller than the one being considered. The proof of the theorem when $k = 1$ is the same as the proof of the general inductive step, and so need not be considered separately. Having fixed k, let $f_1, \cdots, f_k$ be any elements of $\mathfrak{A}$. Let $Q^i{}_\alpha$, $1 \leqq i \leqq k - 1$, be the set of all p in M_α such that the dimension on the manifold M_α of $\mathfrak{A} \cup B_\alpha \cup \{h^1{}_\alpha, \cdots, h^{k-1}{}_\alpha\}$ over B_α at p is i. By the induction hypothesis, the set G_0 of all $(g_1, \cdots, g_{k-1})$ in ${}^{k-1}\mathfrak{A}$ such that for each α, each i $(1 \leqq i \leqq k - 1)$, and each p in $Q^i{}_\alpha$ the dimension on the manifold M_α at p

of $B \cup \{g_1 + h^1{}_\alpha, \cdots, g_{k-1} + h^{k-1}{}_\alpha\}$ over B_α is at least i has the property that ${}^{k-1}\mathfrak{A} - G_0$ is of third category. Fix some $(g_1, \cdots, g_{k-1})$ in G_0. Let Q_α be the set of points p in M_α for which the dimension at p of

$$S_1 = \mathfrak{A} \cup B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_{k-1} + h^{k-1}{}_\alpha\} \cup \{h^k{}_\alpha\}$$

over

$$S_2 = B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_{k-1} + h^{k-1}{}_\alpha\}$$

is at least 1. By Lemma 2, the set Z of g_k in $\mathfrak{A}$ such that for each α and each p in Q_α the dimension at p of $B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_k + h^k{}_\alpha\}$ over $B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_{k-1} + h^{k-1}{}_\alpha\}$ is at least 1 has a complement of first category. We first show that $g = (g_1, \cdots, g_k)$ is in G for each $g_1, \cdots, g_{k-1}$ in G_0 and each g_k in Z. Afterward, we show that this implies that ${}^k\mathfrak{A} - G$ is of third category.

We therefore now prove that $g \in G$. Consider a point p in some $P^i{}_\alpha$. Let λ be the dimension at p of

$$T_1 = \mathfrak{A} \cup B_\alpha \cup \{h^1{}_\alpha, \cdots, h^k{}_\alpha\}$$

and μ that of B_α, so that $\lambda - \mu \geqq i$ because $p \in P^i{}_\alpha$. Let ν be the dimension at p of

$$T_2 = \mathfrak{A} \cup B_\alpha \cup \{h^1{}_\alpha, \cdots, h^{k-1}{}_\alpha\}.$$

Then either $\lambda = \nu$ or $\lambda = \nu + 1$ (see [10], p. 43), since T_1 contains one more function than T_2. Consider first the case $\nu = \lambda$ and $i < k$. Then $\nu - \mu \geqq i$, so that $p \in Q^i{}_\alpha$. Therefore the dimension at p of $B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_{k-1} + h^{k-1}{}_\alpha\}$ over B_α is at least i. Therefore g satisfies (*) at the point p.

Next consider the case in which either $\nu = \lambda - 1$ or $i = k$. Thus $\nu - \mu \geqq i - 1$, so that $p \in Q^{i-1}{}_\alpha$ if $i \neq 1$.

Therefore the dimension at p of $B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_{k-1} + h^{k-1}{}_\alpha\}$ over B_α is at least $i - 1$; this clearly also holds if $i = 1$. Thus to show that g satisfies (*) at the point p it is enough to show that the dimension at p of $B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_k + h^k{}_\alpha\}$ over $B_\alpha \cup \{g_1 + h^1{}_\alpha, \cdots, g_{k-1} + h^{k-1}{}_\alpha\}$ is at least 1. Therefore it is enough to show that $p \in Q_\alpha$, or that the dimension of S_1 over S_2 is at least 1 at p. Consider first the case $\nu = \lambda - 1$. Now the level sets of S_1 and $S_2 \cup \mathfrak{A}$ are the same as the level sets of T_1 and T_2 respectively, because $g_1, \cdots, g_{k-1}$ are in $\mathfrak{A}$. Thus the dimension at p of S_1 over S_2 is at least $\lambda - \nu = 1$, so that $p \in Q_\alpha$ and g therefore satisfies (*) at the point p. Consider next the case $\lambda = \nu$ and $i = k$. Then $\lambda \geqq \mu + i = \mu + k$, and as above we see that λ is the dimension of S_1 at p. Since S_2 contains $k - 1$ more functions than B_α and since B_α has dimension μ at p, the dimension of S_2 at p is at most $\mu + (k-1)$. Therefore the dimension of S_1 over S_2 at p is at least $\mu + k - (\mu + k - 1) = 1$. Thus $p \in Q_\alpha$ so that g satisfies condition (*) at the point p in this case and therefore in all cases. It follows that $(g_1, \cdots, g_k) \in G$.

To see now that ${}^{k}\mathfrak{A} - G$ is of third category in ${}^{k}\mathfrak{A}$, note that ${}^{k-1}\mathfrak{A} - G_0$ is of third category in ${}^{k-1}\mathfrak{A}$ and for each $(g_1, \cdots, g_{k-1})$ in G_0 the set of $\tilde{g}_k$ in $\mathfrak{A}$ with $(g_1, \cdots, \tilde{g}_k)$ in ${}^{k}\mathfrak{A} - G$ is a subset of $\mathfrak{A} - Z$ and therefore of first category in $\mathfrak{A}$. Therefore ${}^{k}\mathfrak{A} - G$ is of third category, as was to be proved.

3. Analytic polyhedra and weak holomorphic convexity.

In this section we investigate mappings of a d-dimensional partially analytic space into C^d. Theorem 1 of the last section of course has applications to such mappings, but the purpose of this section is to obtain stronger results, under the assumption that K has certain analytic convexity properties. The basic notion is that of an analytic polyhedron.

Definition 5. A subset L of a partially analytic space K is called *central* if it is the union of some subfamily of the family of structure manifolds of K and if each component of an open set in L is open. Let $(f_1, \cdots, f_n)$ be functions in $\mathfrak{A}$ and let L be a central subset of K. Define

$$P_0 = \{p \colon p \in L, |f_i(p)| < 1, 1 \leqq i \leqq n\}.$$

Let P be a union of certain components of P_0. If the closure $\bar{P}$ of P is a compact subset of L, then P is called an *analytic polyhedron* defined by the functions $(f_1, \cdots, f_n)$, and L is called the *frame* of P. The *dimension* of P is the maximum of the dimensions of $\mathfrak{A}$ on the manifolds $M_\alpha \cap P$ for $M_\alpha \subset L$. P is called *reduced* if $n \leqq \dim P$; otherwise U is called *unreduced*. An unreduced analytic polyhedron P is called *prepared* if for each structure manifold M_α of K which is a subset of L and intersects P the set $\mathfrak{A}$ has dimension 0 on the manifold $M_\alpha \cap P \cap \{p \colon f_1(p) \neq 0\}$ over the set $\{f_2(f_1)^{-1}, \cdots, f_n(f_1)^{-1}\}$. Bdry P denotes the boundary of P when P is considered as a subset of its frame L.

Note that an analytic polyhedron P is an open subset of its frame L, since each component of the open set P_0 in L is open in L. Therefore $\operatorname{bdry} P = \bar{P} - P$.

LEMMA 3. *If P is an analytic polyhedron defined by $f_1, \cdots, f_n$, then for each p in* bdry P *there exists k, $1 \leqq k \leqq n$, with $|f_k(p)| = 1$.*

Proof. Let P_0 be defined as above. Assume the lemma is not true. Then $|f_i(p)| < 1$, $1 \leqq i \leqq n$, so that $p \in P_0$. Since P is both open and closed in P_0, and since $p \in \operatorname{bdry} P \subset P$, it follows that $p \in P$. This contradiction shows that the lemma is true.

THEOREM 2. *Let K be a partially analytic space and let $f_1, \cdots, f_n$ be functions in $\mathfrak{A}$ defining an analytic polyhedron P with frame L. Let S be a compact subset of P and $r > 1$ a constant such that*

$$S \subset P \cap \{p : |f_i(p)| < r^{-1}, 1 \leqq i \leqq n\}.$$

For each positive integer N let Q be the union of those components of

$$Q_0 = \{p : p \in L, |(rf_1(p))^N| < 1, |(rf_i(p))^N - (rf_1(p))^N| < 1, 2 \leqq i \leqq n\}$$

which contain points of S. Let R be the union of those components of

$$R_0 = \{p : p \in L, |(rf_i(p))^N - (rf_1(p))^N| < 1, 2 \leqq i \leqq n\}$$

which contain points of S. If N is sufficiently large, then Q is an analytic polyhedron with frame L and $S \subset Q \subset P$. If P is prepared and if N is sufficiently large, then R is an analytic polyhedron with frame L and $S \subset R \subset P$.

Proof. Clearly $S \subset Q$ and $S \subset R$ if N is chosen so large that $|f_i(p)| < \frac{1}{2} r^{-N}$, $1 \leqq i \leqq n$, $p \in S$. Clearly, also, the fact that Q and R are analytic polyhedra with frame L will follow from the inclusions $Q \subset P$ and $R \subset P$. Consider first the general case, so that P need not be prepared. We wish to prove $Q \subset P$. Now if p is any point in $\operatorname{bdry} P$, then $|f_i(p)| = 1$ for some i. If $|f_1(p)| \geqq r^{-1}$, then by the definition of Q_0 it is clear that p is not in Q. If $|f_1(p)| < r^{-1}$, then

$$|(rf_i(p))^N - (rf_1(p))^N| \geqq r^N - (rr^{-1})^N = r^N - 1,$$

so that p is not in Q is N is sufficiently large. Thus if N is sufficiently large Q does not intersect $\operatorname{bdry} P$. Thus each component of Q is either a subset of P or disjoint from P. Since each component of Q intersects $S \subset P$, it follows that $Q \subset P$, as was to be proved.

Now assume that P is prepared. We must show that $R \subset P$ if N is sufficiently large. To this end it suffices as above to show that R does not intersect $\operatorname{bdry} P$. Assume therefore that $(\operatorname{bdry} P) \cap R$ is non-void for a sequence $\{N_m\}$ of values of N, where $N_m \rightarrow \infty$ as $m \rightarrow \infty$. Choose a constant c with $r^{-1} < c < 1$ and write

$$T^0{}_m = R \cap P - V,$$

where

$$V = \{p : |f_i(p)| < c, 1 \leqq i \leqq n\}.$$

Since $(\operatorname{bdry} P) \cap R$ is non-void, there exists a component G of $R - V$ which intersects $\operatorname{bdry} P$. Now G contains a point q_0 of the boundary (in L) of $V \cap L$, since otherwise G would be a component of R containing no points of S. Let T_m be the component of $T^0{}_m$ containing q_0, so that $T_m \subset G$. Now T_m intersects $\operatorname{bdry} P$, for otherwise T_m would be a component of $R - V$ and would therefore equal G, contradicting the fact that G contains a point of $\operatorname{bdry} P$. For each p in T_m there exists k, $1 \leqq k \leqq n$, with $|f_k(p)| \geqq c$. For this value of k we have

$$r^N |f_1(p)|^N \geqq |(rf_k(p))^N| - |(rf_k(p))^N - (rf_1(p))^N| \geqq (cr)^N - 1,$$

where $N = N_m$. Hence, for $p \in T_m$, $f_1(p) \neq 0$ and

$$|(f_i(p))^N (f_1(p))^{-N} - 1| < ((cr)^N - 1)^{-1} < 2(cr)^{-N}$$

if $N = N_m$ is sufficiently large. Let D_m consist of all complex numbers z such that $|z^N - 1| < 2(cr)^{-N}$. For z in D_m,

$$1 - 2(cr)^{-N} < |z|^N < 1 + 2(cr)^{-N},$$

so that

$$1 - 2(cr)^{-N} < |z| < 1 + 2(cr)^{-N},$$

or $|1 - |z|| < 2(cr)^{-N}$. Also, if $\arg z^N$ is chosen between $-\pi$ and π, then $|z^N - 1| \geqq \frac{1}{2} |\arg z^N|$, so that $|\arg z^N| \leqq 4(cr)^{-N}$. There therefore exists an integer j, $0 \leqq j \leqq N - 1$, such that

$$|\arg z - 2j\pi N^{-1}| \leqq 4N^{-1}(cr)^{-N} < 4(cr)^{-N}$$

if $\arg z$ is chosen properly. Thus, if $\zeta^j = \exp(2\pi(-1)^{\frac{1}{2}} j N^{-1})$, we have

$$\begin{aligned} |z - \zeta^j| &\leqq ||z| - |\zeta^j|| + |\arg z - \arg \zeta^j| \\ &\leqq 2(cr)^{-N} + 4(cr)^{-N} = 6(cr)^{-N}. \end{aligned}$$

Therefore D_m is contained in the union of the circular neighborhoods of radii $6(cr)^{-N}$ about the N_m-th roots of unity. These neighborhoods are clearly disjoint if N_m is sufficiently large. Thus the functions $f_i(f_1)^{-1}$, $2 \leqq i \leqq n$, each map T_m into the union of these disjoint neighborhoods. Since T_m is connected, $f_i(f_1)^{-1}$ maps T_m into a particular such neighborhood F_{mi}. Let the corresponding N_m-th root of unity be $\zeta_{m,i}$. Thus

$$|f_i(p)(f_1(p))^{-1} - \zeta_{m,i}| < 6(cr)^{-N_m}$$

for all p in T_m. By passing to a subsequence of $\{N_m\}$ if necessary, we may assume that $\{\zeta_{m,i}\}$ converges for each i to a number ζ_i as $m \to \infty$. The sequence $\{T_m\}$ of compact subsets of the compact set P may also be assumed to converge to a compact subset T of P, in the usual topology for compact subsets of a compact space. T_m is connected because T_m is connected, so that T is connected. Clearly T is a closed subset of P. Since T_m contains points in bdry P and bdry V, T also contains points in bdry P and bdry V. Also

$$f_i(p)(f_1(p))^{-1} = \zeta_i, \qquad 2 \leqq i \leqq n,$$

for all p in T. Partition T into equivalence classes by defining $p \equiv q$, for p and q in T, to mean $f_i(q) = f_i(p)$, $1 \leqq i \leqq n$. Since T is connected and contains points in bdry P and bdry V, since each f_i is bounded in absolute value by $c < 1$ on bdry V, and since to each point in bdry P there exists f_i having absolute value 1 at that point, it follows that some f_i assumes an uncountable number of values on the set $T \cap P$. Therefore there are an uncountable number of partition classes of $T \cap P$. Thus there exist an $M_\alpha \subset L$ such that M_α intersects an uncountable number of partition classes of $T \cap P$. Let S be that level set of the functions $f_2(f_1)^{-1}, \cdots, f_n(f_1)^{-1}$ on $P \cap M_\alpha \cap \{p : f_1(p) \neq 0\}$ which contains the set $T \cap P$, so that S contains an uncountable number of level sets of $f_1, \cdots, f_n$ on M_α. The locally analytic set S in M_α splits into a countable family $\{S_k\}$ of irreducible analytic sets, none of which is a subset of the union of the others. There exists k_0 such that $f_1, \cdots, f_n$ are not all constant on S_{k_0}. Since S_{k_0} is irreducible the sets of constancy of $f_1, \cdots, f_n$ on S_{k_0} are all of dimension less than the dimension of S_{k_0}. If p_0 is a point in S_{k_0} not in any of the other S_k, it follows that the dimension on the manifold M_α of $f_1, \cdots, f_n$ over $f_2(f_1)^{-1}, \cdots, f_n(f_1)^{-1}$ at p_0 is at least 1, contradicting the fact that P is prepared. This completes the proof.

LEMMA 4. *Let $\{L_j\}$ be a finite family of central subsets of a partially analytic space K, and let $f_1, \cdots, f_n$ be functions in $\mathfrak{A}$ such that for each j there exists an integer $\gamma = \gamma(j)$, $1 \leqq \gamma(j) \leqq n$, such that $f_1, \cdots, f_\gamma$ define an analytic polyhedron P_j with frame L_j. For each j let S_j be a compact subset of P_j. Then there exist functions $f'_1, \cdots, f'_n$ in $\mathfrak{A}$ such that for each j the functions $f'_1, \cdots, f'_\gamma$ define an analytic polyhedron P'_j with frame L_j with*

$$S_j \subset P'_j \subset P_j$$

such that P'_j is unreduced and prepared if P_j is unreduced.

Proof. Choose $\epsilon > 0$ such that

$$S_j \subset P_j \cap \{p : |f_i(p)| < 1 - 2\epsilon, 1 \leqq i \leqq \gamma(j)\}$$

for all values of j. Consider a value of j for which P_j is unreduced and let M_α be any structure manifold which intersects P_j and is a subset of L_j. Let

$$N_{j\alpha} = P_j \cap M_\alpha \cap \{p : f_1(p) \neq 0\}.$$

The dimension of $\mathfrak{A}$ on $N_{j\alpha}$ is less than γ, since P_j is unreduced. Since the level sets of $\mathfrak{A}$ are the same as the level sets of

$$H = \mathfrak{A} \cup \{f_2(f_1)^{-1}, \cdots, f_n(f_1)^{-1}\},$$

the dimension of H on $N_{j\alpha}$ is at most $\gamma - 1$. Let G_j be the set of all $(g_2, \cdots, g_n)$ in ${}^{n-1}\mathfrak{A}$ such that for all α the set H has dimension 0 on the manifold $N_{j\alpha}$ over the set

$$D = \{g_2 + f_2(f_1)^{-1}, \cdots, g_\gamma + f_\gamma(f_1)^{-1}\},$$

and let $G = \bigcap_j G_j$. By Theorem 1, with B_α the void set, ${}^{n-1}\mathfrak{A} - G_j$ is of third category in ${}^{n-1}\mathfrak{A}$. Thus the set

$${}^{n-1}\mathfrak{A} - G = \bigcup_j ({}^{n-1}\mathfrak{A} - G_j)$$

is of third category in ${}^{n-1}\mathfrak{A}$, where the union is taken over all j for which P_j is unreduced. Thus there exists $(g_2, \cdots, g_n)$ in G such that for all j we have $|g_i(p)| < \epsilon$ whenever $2 \leqq i \leqq \gamma(j)$ and $p \in P_j$, whether or not P_j is unreduced. Define

$$f'_i = (1-\epsilon)^{-1}[g_i f_1 + f_i], \qquad 2 \leqq i \leqq n,$$

and $f'_1 = f_1$. Since the level sets of $\mathfrak{A}$ are the same as the level sets of H, we see by the above that $\mathfrak{A}$ has dimension 0 over the set

$$\{f'_2(f'_1)^{-1}, \cdots, f'_\gamma(f'_1)^{-1}\} = (1-\epsilon)^{-1}D$$

on the manifolds $N_{j\alpha}$ for each j for which P_j is unreduced. For each j let P'_j be the union of those components of

$$P''_j = \{p : p \in L_j, |f'_i(p)| < 1, 1 \leqq i \leqq \gamma(j)\}$$

which intersect S_j. For each p in S_j and for $2 \leqq i \leqq \gamma$, we have

$$f'_i(p) \leqq (1-\epsilon)^{-1}[\epsilon\,|f_1(p)| + |f_i(p)|] \leqq (1-\epsilon)^{-1}(1+\epsilon)(1-2\epsilon) < 1.$$

Clearly also $|f'_1(p)| < 1$ for p in S_j. Therefore $S_j \subset P''_j$ and hence $S_j \subset P'_j$. Consider now p in $\operatorname{bdry} P_j$. By Lemma 3, $|f_i(p)| = 1$ for some i, $1 \leqq i \leqq \gamma$. If $i = 1$, then clearly p is not in P'_j. If $2 \leqq i \leqq \gamma$, then

$$|f'_i(p)| \geqq (1-\epsilon)^{-1}[|f_i(p)| - |f_1(p)|\,|g_i(p)|] \geqq (1-\epsilon)^{-1}(1-\epsilon) = 1,$$

so that $p \notin P'_j$ in this case also. Thus P'_j does not intersect $\operatorname{bdry} P_j$. Since each component of P'_j contains a point of $S_j \subset P_j$, it follows that $P'_j \subset P_j$. Thus P'_j is an analytic polyhedron with frame L_j defined by $f'_1, \cdots, f'_\gamma$. If P_j is unreduced then P'_j is also unreduced since $P'_j \subset P_j$ implies $\dim P'_j$

$\leqq \dim P_j$; P'_j is also prepared since we have seen that $\mathfrak{A}$ has dimension 0 over $f'_2(f'_1)^{-1}, \cdots, f'_\gamma(f'_1)^{-1}$ on each of the manifolds

$$N_{j\alpha} \supset P'_j \cap M_\alpha \cap \{p : f'_1(p) \neq 0\}$$

This completes the proof.

THEOREM 3. *Let $\{L_j\}$ be a finite family of central subsets of the partially analytic space K. Let the functions $f_1, \cdots, f_n$ in $\mathfrak{A}$ define for each j an analytic polyhedron P_j with frame L_j. Let $\gamma = \gamma(j) = \min\{n, \dim P_j\}$. Let S_j be a compact subset of P_j. Then there exist functions $f'_1, \cdots, f'_n$ in $\mathfrak{A}$ such that for each j the functions $f'_1, \cdots, f'_\gamma$ define an analytic polyhedron P'_j with frame L_j such that $S_j \subset P'_j \subset P_j$.*

Proof. Let T be the class of all positive integers m such that there exist $h_1, \cdots, h_n$ in $\mathfrak{A}$ such that for each j the functions $h_1, \cdots, h_\delta$ define an analytic polyhedron Q_j with frame L_j with $S_j \subset Q_j \subset P_j$, where $\delta = \delta(j) = \max\{\gamma(j), m\}$. Clearly the set T is non-void, since by hypothesis $n \in T$. Clearly also the lemma will be proved if it is shown that $1 \in T$. To this end, assume $1 \notin T$. Let m be the least integer in T, and choose $h_1, \cdots, h_n$ as above. We will prove that $m - 1 \in T$ and thus obtain a contradiction. The polyhedra Q_j with $\gamma(j) < m$ are unreduced, since $\dim Q_j \leqq \dim P_j = \gamma(j)$. Therefore, by applying Lemma 4, we may assume that the polyhedra Q_j with $\gamma(j) < m$ are prepared. Let $r > 1$ be such that $|h_i(p)| < r^{-1}$, $1 \leqq i \leqq \gamma(j)$, $p \in S_j$, for all values of j. We define

$$\begin{aligned} h'_1 &= (rh_2)^N - (rh_1)^N, \\ &\;\vdots \\ h'_{m-1} &= (rh_m)^N - (rh_1)^N, \\ h'_m &= (rh_1)^N, \\ h'_{m+1} &= (rh_{m+1})^N - (rh_1)^N \\ &\;\vdots \\ h'_n &= (rh_n)^N - (rh_1)^N. \end{aligned}$$

If N is sufficiently large it follows from Theorem 2 that $h'_1, \cdots, h'_\beta$ define an analytic polyhedron Q'_j with frame L_j such that $S_j \subset Q'_j \subset Q_j \subset P_j$, where $\beta = \max\{\gamma(j), m - 1\}$. This shows that $m - 1 \in T$. From this contradiction we conclude that $1 \in T$, as was to be proved.

Definition 6. A partially analytic space K is called *weakly holomor-*

phically convex if it is the union of its structure manifolds and if for each compact $S \subset K$ each component of the set

$$\hat{S} = \{p : p \in K, |f(p)| \leqq \max_{q \in S} |f(q)|, \text{ all } f \text{ in } \mathfrak{A}\}$$

is compact.

Definition 7. A continuous mapping ϕ of a topological space T_1 into a topological space T_2 is *almost proper* if each component of $\phi^{-1}(S)$ is compact for each compact subset S of T_2.

THEOREM 4. *Let $\{L_j\}$ be a finite family of closed central subsets of a weakly holomorphically convex partially analytic space K. Let the dimensions of $\mathfrak{A}$ on the structure manifolds of K be bounded and have the maximum value n. Let $\gamma = \gamma(j)$ be the maximum of the dimensions of $\mathfrak{A}$ on the structure manifolds of K which are subsets of L_j. Then the set of elements $f = (f_1, \cdots, f_n)$ in ${}^n\mathfrak{A}$ such that for each j the mapping*

$$f^j : p \rightarrow (f_1(p), \cdots, f_\gamma(p))$$

of L_j into C^γ is almost proper is dense in ${}^n\mathfrak{A}$.

Proof. It is permissible to assume that $L_1 = K$. Let $\{S_i\}$ be a sequence of compact sets whose union is K with $S_i \subset \operatorname{interior} S_{i+1}$. Let T_i be an open set containing S_i whose closure is compact and whose boundary does not intersect $\hat{S}_i$. For each point p in bdry T_i, there exists h in $\mathfrak{A}$ with

$$|h(p)| > 1 > \max_{q \in S_i} |h(q)|.$$

By the compactness of bdry T_i, there therefore exist a finite number $h_1, \cdots, h_m$ of functions in $\mathfrak{A}$ such that $|h_k(q)| < 1$ for q in S_i and $1 \leqq k \leqq m$ and such that $|h_k(p)| > 1$ for at least one k if $p \in \operatorname{bdry} T_i$. If we let Q be the union of those components of

$$Q_0 = \{p : p \in K, |h_i(p)| < 1, 1 \leqq i \leqq m\}$$

which intersect S_i, it follows that Q is an analytic polyhedron with frame K and $S_i \subset Q$. Thus $Q \cap L_j$ is an analytic polyhedron with frame L_j, defined by the functions $h_1, \cdots, h_m$, and $S_i \cap L_j \subset Q \cap L_j$. It follows from Theorem 3 that there exist $g^i{}_1, \cdots, g^i{}_n$ in $\mathfrak{A}$ such that for each j the functions $g^i{}_1, \cdots, g^i{}_\gamma$ define an analytic polyhedron Q_{ij} with frame L_j such that $S_i \cap L_j \subset Q_{ij}$. If we construct the Q_{ij} by induction on i, we may assume, by increasing the size of S_{i+1} if necessary, that $\bigcup_j \bar{Q}_{ij} \subset S_{i+1}$. Let $\lambda_1, \cdots, \lambda_n$ be given functions in $\mathfrak{A}$. We show that if the complex constants $\{a_i\}$ and the positive integers $\{t_i\}$ are chosen properly then the functions f_k defined by the series

$$f_k = \sum_{i=1}^{\infty} a_i (g^i{}_k)^{t_i} + \lambda_k, \qquad 1 \leqq k \leqq n,$$

have the required properties and that f_k is arbitrarily close to λ_k in $\mathfrak{A}$.

To this end, write

$$f^m{}_k = \sum_{i=1}^{m} a_i (g^i{}_k)^{t_i} + \lambda_k, \qquad 1 \leqq k \leqq n, 1 \leqq m < \infty.$$

Let m_0 be an arbitrary positive integer. Choose $a_1, \cdots, a_{m_0}$ to be zero and $t_1, \cdots, t_{m_0}$ to be 1. We now give the rules for choosing a_m and t_m, assuming that the previous a_i and t_i have been chosen. Choose

$$|a_m| > \max\{|f^{m-1}{}_k(p)| : 1 \leqq k \leqq \gamma(j), p \in \operatorname{bdry} Q_{mj}, \text{all } j\} + m + 1.$$

Then choose t_m so large that

$$\max\{|a_m(g^m{}_k(p))^{t_m}| : 1 \leqq k \leqq \gamma(j), p \in \bar{Q}_{sj}, s < m, \text{all } j\} < 2^{-m}.$$

This can be done since for $s < m$ we have

$$\bar{Q}_{sj} \subset S_{s+1} \cap L_j \subset S_m \cap L_j \subset Q_{mj}$$

so that $|g^m{}_k(p)| < 1$ for $p \in \bar{Q}_{sj}$ and $k \leqq \gamma(j)$. The sequences $\{a_m\}$ and $\{t_m\}$ having been chosen in this way, we show first that the series defining the functions f_k converge uniformly on compact subsets of K, so that f_k is well-defined and belongs to $\mathfrak{A}$. It is clearly sufficient to consider the compact sets $\bar{Q}_{s1} \supset S_s$. Now $|a_m(g^m{}_k(p))^{t_m}| \leqq 2^{-m}$ for $m > s$ and p in $\bar{Q}_{s1}$, so that the series for f_k converges uniformly on $\bar{Q}_{s1}$. Therefore $f_k \in \mathfrak{A}$. To see that the mapping f^j is almost proper, consider a compact set $H \subset C^\gamma$. It is clearly sufficient to assume that

$$H = \{(z_1, \cdots, z_\gamma) : |z_i| \leqq \alpha, 1 \leqq i \leqq \gamma\}$$

for some $\alpha > 0$. Let Γ be any component of $(f^j)^{-1}(H)$. Choose i such that $\Gamma \cap Q_{ij}$ is non-void. Choose a positive integer m larger than α, i, and m_0. Then $|g^m{}_k(p)| = 1$ for some k, $1 \leqq k \leqq \gamma(j)$, if $p \in \operatorname{bdry} Q_{mj}$. Therefore

$$\begin{aligned} |f_k(p)| &= |f^{m-1}{}_k(p) + \sum_{r=m+1}^{\infty} a_r(g^r{}_k(p))^{t_r} + a_m(g^m{}_k(p))^{t_m}| \\ &\geqq |a_m| - |f^{m-1}{}_k(p)| - \sum_{r=m+1}^{\infty} |a_r(g^r{}_k(p))^{t_r}| \geqq m + 1 - \sum_{r=m+1}^{\infty} 2^{-r} \geqq m > \alpha. \end{aligned}$$

Thus we see that $(f^j)^{-1}(H)$ does not intersect $\operatorname{bdry} Q_{mj}$. We therefore have $\Gamma \subset Q_{mj}$. Thus Γ is a closed subset of the compact set $\bar{Q}_{mj}$. Therefore Γ is compact. It follows that f^j is almost proper, as was to be proved. It is also clear that f_k can be made arbitrarily close to λ_k by taking m_0 sufficiently large.

4. Special analytic polyhedra and integration.

In order to study the local properties of an analytic ployhedron, it is helpful to impose certain restrictions.

Definition 8. A reduced analytic polyhedron P in a partially analytic space K with frame L defined by functions $f_1, \cdots, f_n$ in $\mathfrak{A}$ will be called *special* if the level sets of $f_1, \cdots, f_n$ on P are countable and if the set Λ of all α such that $M_\alpha \subset L$, M_α intersects P, and $\dim M_\alpha = n$ has the property that $(\bigcup_{\alpha \in \Lambda} M_\alpha) \cap P$ is dense in P and that $M_\alpha \cap P$ is open in L for each α in Λ.

It is clear that each component of a special analytic polyhedron is a special analytic ployhedron.

Definition 9. If X is a topological space we define ${}_kX$, called the k-fold *unordered product* of X with itself, to be the set of all unordered k-tuples of elements of X. The natural map of the k-fold Cartesian product ${}^kX$ of X with itself into ${}_kX$ is denoted by Ω_X, or $\Omega^k{}_X$ if k is not clear from the context. A set in ${}_kX$ is defined to be *open* if and only if its inverse image under the map Ω_X is an open set in ${}^kX$.

It is clear that ${}_kX$ is Hausdorff if X is Hausdorff and compact if X is compact.

THEOREM 5. *Let P be a special analytic polyhedron with frame L in a partially analytic space K defined by the functions $f_1, \cdots, f_n$ in $\mathfrak{A}$. Let E^n be the subset of C^n consisting of points whose coordinates are less than* 1 *in absolute value, and let f be the map*

$$p \rightarrow (f_1(p), \cdots, f_n(p))$$

of P into E^n. For each α in Λ let $M^\alpha{}_1$ be the subset of M_α consisting of all points in $M_\alpha \cap P$ at which $(f_1, \cdots, f_n)$ is a coordinate set of functions. Then the set $M_1 = \bigcup_\alpha M_1{}^\alpha$ is dense in P and $H = f(P - M_1)$ is closed and nowhere dense in E^n. There exists an integer $\lambda \geqq 1$, called the multiplicity of P, such that for each z in $E^n - H$ there exist exactly λ distinct points p in M_1 with $f(p) = z$. The map ω from $E^n - H$ into ${}_\lambda P$ which takes z into the unordered λ-tuple of such points can be uniquely extended to a continuous map ω of E^n into ${}_\lambda P$. The set P has only a finite number of components.

Proof. If $\alpha \in \Lambda$ the set $M_2{}^\alpha = (M_\alpha \cap P) - M_1{}^\alpha$ is a locally analytic subset of M_α, since locally it is given by the vanishing of a certain Jacobian. Also $M_2{}^\alpha \neq M_\alpha \cap P$ because $M_2{}^\alpha = M_\alpha \cap P$ would imply that locally one of the functions $f_1, \cdots, f_n$ depends on the others, contradicting the fact that the level sets of $f = (f_1, \cdots, f_n)$ on $M_\alpha \cap P$ are countable. Thus $M_2{}^\alpha$ is the union of a finite family $\{N^\alpha{}_\beta\}$ of analytic submanifolds of M_α, with $\dim N^\alpha{}_\beta < \dim M_\alpha = n$. Since $M_1{}^\alpha$ is clearly dense in M_α and $\bigcup_{\alpha \in \Lambda} M_\alpha$ is dense in P, M_1 is dense in P. Now each $N^\alpha{}_\beta$ is a countable union of closed sets, as is each $M_\alpha \cap P$, $\alpha \notin \Lambda$. Thus $f(N^\alpha{}_\beta)$, $\alpha \in \Lambda$, and $f(M_\alpha \cap P)$, $\alpha \notin \Lambda$ are countable unions of closed sets of topological dimensions $\leqq 2n - 2$, since the analytic image of a closed set of dimensions $\leqq 2n - 2$ is of dimension $\leqq 2n - 2$. It follows that real $\dim H \leqq 2n - 2$. Therefore $E^n - H$ is connected (see [7] for these theorems). Since $f(M_1)$ is of real dimension $2n$, $f(M_1) - H$ is non-void.

For each z in $E^n - H$ let $I(z)$ be the number of points p in M_1 with $f(p) = z$. If $I(z)$ were not finite, the set of such points p would have a limit point p_0 in $\bar{P}$. Actually p_0 is in P, since $f(p_0) \in E^n$ implies by Lemma 3 that p_0 is not in bdry P. If $p_0 \in M_\alpha$ for some $\alpha \in \Lambda$, the fact that $M_\alpha \cap P$ is open in P implies that the level set of f on M_α containing p_0 also contains the points p which are sufficiently near to p_0. Thus this level set has p_0 as a limit point and is therefore not 0-dimensional; it is therefore uncountable, contradicting the fact that P is a special analytic polyhedron. Thus p_0 is not in $M_1 \subset \bigcup_{\alpha \in \Lambda} M_\alpha$. Also p_0 is not in $P - M_1$ since z is not in H. Thus p_0 is not in P at all. This contradiction shows that $I(z)$ is finite. For each positive integer γ let

$$T_\gamma = \{z : z \in E^n - H, I(z) \geqq \gamma\}.$$

If $z_0 \in T_\gamma$, there are distinct points $p_1, \cdots, p_\gamma$ in M_1 with $f(p_i) = z_0$. Choose α_i in Λ with $p_i \in M_1{}^{\alpha_i}$. For each i, $1 \leqq i \leqq \gamma$, the functions $f_1, \cdots, f_n$ are a coordinate set at p_i on the manifold $M_1{}^{\alpha_i}$. There therefore exist coordinate neighborhoods $U_1, \cdots, U_\gamma$ of these points. Thus $f(U_i)$ is a neighborhood V_i of z_0 in E^n and if $z \in \cap V_i$, there exists q_i in U_i, $1 \leqq i \leqq \gamma$, with $f(q_i) = z$. It follows that $I(z) \geqq \gamma$. Thus T_γ is an open set in $E^n - H$.

To see that T_γ is closed in $E^n - H$, consider z_0 in $\bar{T}_\gamma \cap (E^n - H)$. Let $\{z_j\}$ be a sequence of points in T_γ converging to z_0. Let $p^1{}_j, \cdots, p^\gamma{}_j$ be distinct points in M_1 with $f(p^i{}_j) = z_j$. We may assume that for each i, $1 \leqq i \leqq \gamma$, the sequence $\{p^i{}_j\}$ converges to a point p^i in $\bar{P}$. Clearly $f(p^i) = z_0$, so as above we have $p^i \in P$. Since $z_0 \in E^n - H$, $p^i \in M_1$. If the points p^i, $1 \leqq i \leqq \gamma$, are not distinct, for instance if $p^1 = p^2$, then $p^1{}_j$ and $p^2{}_j$ are distinct points which are arbitrarily near to p^1 at which f assumes the same values.

Thus f is not one-to-one on any neighborhood of p^1, contradicting the fact that $p^1 \in M_1$. Thus the points p^i, $1 \leqq i \leqq \gamma$, are distinct. Therefore $z \in T_\gamma$. Thus T_γ is both open and closed in $E^n - H$. Since $E^n - H$ is connected it follows that either T_γ is void or $T_\gamma = E^n - H$. Now T_γ is certainly void for some integer γ; take γ larger than $I(z)$ for some z in $E^n - H$. Let λ be the greatest integer such that T_λ is not void. It is clear that $I(z) \geqq \lambda$ for all z, since $T_\lambda = E^n - H$. If $I(z) > \lambda$ for some z, then $T_{\lambda+1}$ is non-void, contradicting the choice of λ. Therefore $I(z) = \lambda$ for all z in $E^n - H$. This integer λ is called the multiplicity of the analytic polyhedron P.

To see that H is closed in E^n, for each $r < 1$ let

$$P_r = P \cap \{p : |f_i(p)| < r, 1 \leqq i \leqq n\}.$$

Now M_1 is open in P since each M_1^α is open in P. Thus $P_r - M_1$ is compact. Therefore $f(P_r - M_1)$ is closed in E^n. But

$$f(P_r - M_1) = f(P - M_1) \cap \{(z_1, \cdots, z_n) \in E^n : |z_i| < r, 1 \leqq i \leqq n\}.$$

It follows that $H = f(P - M_1)$ is closed in E^n.

It remains to show that ω is continuous on $E^n - H$ and to extend ω continuously to E^n. The extension of ω will perforce be unique because $E^n - H$ is dense in E^n. To see that ω is continuous on $E^n - H$, let $\{z_i\}$ be a sequence of points in $E^n - H$ converging to a point z_0 in $E^n - H$. Let $\omega(z_i)$ be the unordered λ-tuple $\{p^i{}_1, \cdots, p^i{}_\lambda\}$ in ${}_\lambda P$ and let $\omega(z)$ be $\{p_1, \cdots, p_\lambda\}$. If ω is not continuous on $E^n - H$, the sequence $\{z_i\}$ and the point z_0 can be chosen so that $\omega(z_i)$ converges to a point $\mu \neq \omega(z_0)$ in ${}_\lambda P$. As above we see that μ consists of λ distinct points p in M_1 with $f(p) = z_0$. Therefore $\mu = \omega(z_0)$, a contradiction, proving that ω is continuous on $E^n - H$.

To show that ω can be extended continuously to E^n it is enough, since ${}_\lambda P$ is metrizable, to show that ω has a continuous extension to $(E^n - H) \cup \{z_0\}$ for each z_0 in H. To do this, let $p_1, \cdots, p_k$ be all points in $\bar{P}$ with $f(p_i) = z_0$, so that actually $p_i \in P$, $1 \leqq i \leqq k$. Let $U_1, \cdots, U_k$ be disjoint neighborhoods of $p_1, \cdots, p_k$ respectively. Assume that there exists a sequence $\{z_i\}$ of points converging to z_0 such that for each i there exists a point q_i in $P - U_1 - \cdots - U_k$ with $f(q_i) = z_i$. Then any limit point q of the sequence $\{q_i\}$ has the property that $f(q) = z_0$ and $q \in \bar{P} - U_1 - \cdots - U_k$. This contradiction shows that the seqeunce $\{z_i\}$ does not exist. Therefore

$$f^{-1}(V) \cap P \subset U_1 \cup \cdots \cup U_k$$

if V is a small enough neighborhood of z_0. Since V is open in E^n and real $\dim H \leqq 2n - 2$, the set $V - H$ is connected. For each z in $V - H$ let $\delta_i(z)$,

$1 \leq i \leq k$, be the number of elements in the set $\omega(z) \cap U_i = f^{-1}(z) \cap U_i$. Since ω is continuous on $E^n - H$, δ_i is continuous. Since $V - H$ is connected, δ_i is therefore constant on $V - H$. Clearly $\sum \delta_i = \lambda$. Define $\omega(z_0) \in {}_\lambda P$ to consist of the points $p_1, \cdots, p_k$ with the respective multiplicities $\delta_1, \cdots, \delta_k$. This choice is clearly independent of the neighborhood V, and the extension of ω so defined to $(E^n - H) \cup \{z_0\}$ is clearly continuous at z_0.

To see finally that P has a finite number of components, note that each component of P is itself a special analytic polyhedron, and therefore by the analysis just given contains a point p with $f(p) = 0$. Since by the analysis just given P contains only λ such points p, it follows that actually P has at most λ components.

LEMMA 5. *Let P be a special analytic polyhedron in a partially analytic space K defined by functions $f_1, \cdots, f_n$. Let s be a function on C^λ which is a symmetric polynomial in the variables $(z_1, \cdots, z_\lambda)$ and let $\bar{s}$ be the unique continuous function on ${}_\lambda C$ (where C is the complex plane) such that $\bar{s} \circ \Omega_X = s$. Let g be a continuous function on P. Let ${}_\lambda g$ be the continuous function on ${}_\lambda P$ which takes the unordered λ-tuple $\{p_1, \cdots, p_\lambda\}$ into the point $\{g(p_1), \cdots, g(p_\lambda)\}$ in ${}_\lambda C$. Let $\bar{g} = \bar{s} \circ {}_\lambda g \circ \omega$. Then $\bar{g}$ is a continuous function on E^n which is analytic on E^n if g is analytic on $M_\alpha \cap P$ for each α in Λ.*

Proof. Since g is continuous ${}_\lambda g$ is continuous. Therefore $\bar{g} = \bar{s} \circ {}_\lambda g \circ \omega$ is continuous. Assume that g is analytic on each $M_\alpha \cap P$ for $\alpha \in \Lambda$. Consider any point z in $E^n - H$. There exists a neighborhood U of z such that $f^{-1}(U) \cap P$ is the union of disjoint neighborhoods $U_1, \cdots, U_\lambda$ of the points of $\omega(p)$. We may assume that each U_i lies in some M_α, $\alpha \in \Lambda$, and that U_i is mapped homeomorphically onto U by f. This makes it clear that $\bar{g}$ is analytic at z. Thus $\bar{g}$ is analytic on $E^n - H$. To show that $\bar{g}$ is analytic on E^n, we need only show that $\bar{g}$ is analytic on all one-dimensional coordinate planes. As typical of such coordinate planes, consider the planes

$$L_c = \{z = (z_1, \cdots, z_n) \in E^n : (z_1, \cdots, z_{n-1}) = c = (c_1, \cdots, c_{n-1})\},$$

where c is a point of E^{n-1}. Let G consist of all c in E^{n-1} such that $H \cap L_c$ is countable. Since $\bar{g}$ is continuous on E^n and analytic on $E^n - H$, $\bar{g}$ is analytic on L_c for each c in G. Clearly, then, $\bar{g}$ is analytic on L_c for all c in $\bar{G}$. Thus we need only show that $\bar{G} = E^{n-1}$. To do this we shall show that $E^{n-1} - G$ is of first category in E^{n-1}.

Let $\{U_k\}$ be a countable basis for the open sets in E^1. Let $\{J_\delta\}$ be the family consisting of the manifolds $M_\alpha \cap P$, $\alpha \notin \Lambda$, and $N^\alpha{}_\beta$, $\alpha \in \Lambda$, where the $N^\alpha{}_\beta$ are defined as in Theorem 5. Thus $H \subset \bigcup_\delta f(J_\delta)$. For each δ let $\{G_{\delta\gamma}\}$

be a countable family of open sets in J_δ which have compact closures in J_δ and which cover J_δ. Then

$$H \subset \bigcup_{\delta,\gamma} f(G_{\delta\gamma}).$$

For each δ, each γ, and each positive integer k let

$$F_{\delta\gamma k} = \{c\colon c \in E^{n-1}, \{c\} \times \bar{U}_k \subset f(\bar{G}_{\delta\gamma})\}.$$

The set $F_{\delta\gamma k}$ is closed because $\bar{U}_k$ and $f(\bar{G}_{\delta\gamma})$ are closed. Also $F_{\delta\gamma k}$ has no interior points, since otherwise $f(\bar{G}_{\delta\gamma})$ would have an interior point in E^n, contradicting the fact that real $\dim f(\bar{G}_{\delta\gamma}) \leqq 2n - 2$.

It follows that $Y = \bigcup_{\delta,\gamma,k} F_{\delta\gamma k}$ is of first category in E^{n-1}. To complete the proof we show that $E^{n-1} - G \subset Y$. Consider $c \in E^{n-1} - G$. There exists $G_{\delta\gamma}$ such that $f(G_{\delta\gamma}) \cap L_c$ is uncountable. Thus f_n assumes an uncountable number of distinct values on the analytic subset

$$S = G_{\delta\gamma} \cap f^{-1}(L_c)$$

of $G_{\delta\gamma}$. It follows that $f_n(S)$ contains some open set in E^1, so that $\bar{U}_k \subset f_n(S)$ for some k. Thus $\{c\} \times \bar{U}_k \subset f(G_{\delta\gamma})$, so that $c \in F_{\delta\gamma k}$. Thus $E^{n-1} - G \subset Y$, as was to be proved.

Definition 10. Let K be a partially analytic space and P a special analytic polyhedron in P defined by the functions $f_1, \cdots, f_n$. For $0 < r < 1$ let

$$P_r = P \cap \{p\colon |f_i(p)| < r, 1 \leqq i \leqq n\}.$$

Let $B_r = P_r \cap \{p\colon |f_i(p)| = r, 1 \leqq i \leqq n\}$. Let

$$E^n{}_r = \{(z_1, \cdots, z_n)\colon |z_i| < r, 1 \leqq i \leqq n\}$$

and $V_r = f(B_r) \subset \operatorname{bdry} E^n{}_r$. Let s be the function on C^λ defined by $s(z_1, \cdots, z_\lambda) = z_1 + \cdots + z_\lambda$. If g is a continuous function on P, define $\bar{g}$ as in Lemma 5, so that

$$\bar{g}(z) = g(p_1) + \cdots + g(p_\lambda),$$

where $\omega(z) = \{p_1, \cdots, p_\lambda\}$. Thus $\bar{g}$ is continuous and is analytic if g is analytic on each $M_\alpha \cap P$, $\alpha \in \Lambda$.

Now the linear functional

$$g \to \int_{V_r} \bar{g}(z)\, dz_1 \cdots dz_n$$

is a continuous linear functional in the uniform norm on the space of all continuous functions g on B_r. It follows by the Riesz representation theorem for such linear functionals that there exists a unique finite complex-valued Borel measure μ on B_r such that

$$\int_{B_r} g(p)\,d\mu(p) = \int_{V_r} \bar{g}(z)\,dz_1 \cdots dz_n$$

for all continuous functions g on B_r. The measure $d\mu$ is written $df_1 \cdots df_n$.

We now give an integral formula for special analytic polyhedra which, while trivial, is fundamental.

THEOREM 6. *Under the conditions of Definition* 10, *if g is an analytic function on $M_\alpha \cap P$ for each $\alpha \in \Lambda$ and if $q \in P_r$, then*

$$(2\pi i)^{-n} \int_{B_r} g(p)[f_1(p) - f_1(q)]^{-1} \cdots [f_n(p) - f_n(q)]^{-1} df_1(p) \cdots df_n(p) = \bar{g}(f(q)).$$

Proof. Write $h = g[f_1 - f_1(q)]^{-1} \cdots [f_n - f_n(q)]^{-1}$. The proof depends on computing $\bar{h}$, which is defined on V_r because h is continuous on B_r. Consider z in V_r and let $\omega(z) = \{p_1, \cdots, p_\lambda\}$. Since $f_i(p_j) = z_i$ for all j, where $z = (z_1, \cdots, z_n)$, it follows that

$$\bar{h}(z) = \bar{g}(z)[z_1 - f_1(q)]^{-1} \cdots [z_n - f_n(q)]^{-1}.$$

We therefore have

$$(2\pi i)^{-n} \int_{B_r} h(p)df_1(q) \cdots df_n(p) = (2\pi i)^{-n} \int_{V_r} \bar{g}(z)[z_1 - f_1(q)]^{-1} \cdots [z_n - f_n(q)]^{-1} dz_1 \cdots dz_n.$$

Since $(f_1(q), \cdots, f_n(q)) \in E^n{}_r$ it follows from the n-times iteration of the Cauchy integral formula that this quantity is just $\bar{g}(f(q))$, as was to be proved.

The integral formula of Theorem 6 is apparently only good for representing functions which have equal values at points of P mapping into the same point of E^n. That this is not the case is shown by the following theorem.

THEOREM 7. *With the notation of Lemma* 5 *and Theorem* 6, *let w be any analytic function on P (continuous on P and analytic on $M_\alpha \cap P$ for each $\alpha \in \Lambda$). Let $\bar{w}$ be the function on $P \times P$ defined by*

$$\bar{w}(p, q) = [w(p_2) - w(q)] \cdots [w(p_\lambda) - w(q)],$$

where $\omega(f(p)) = \{p = p_1, \cdots, p_\lambda\}$. Then $\bar{w}$ is continuous on $P \times P$ and analytic in q for each value of p and analytic in p for each value of q. If w

is in $\mathfrak{A}$, *then* $\tilde{w}(p,q)$ *is in* $\mathfrak{A}$ *when considered as a function of* q *for each fixed* p *in* P. *For each function* g *analytic on* P *and each* q *in* P_r

$$(2\pi i)^{-n}\int_{B_r} g(p)\tilde{w}(p,q)[f_1(p)-f_1(q)]^{-1}\cdots[f_n(p)-f_n(q)]^{-1}df_1(p)\cdots df_n(p)$$
$$=\hat{w}(q)g(q),$$

where the function $\hat{w}(q)=\tilde{w}(q,q)$ *is analytic on* P.

Proof. Clearly

$$\tilde{w}(p,q)=\sum_{i=0}^{\lambda-1}\pm a_i(p)[w(q)]^i,$$

where $a_i(p)$ is the $\lambda-i-1$-th elementary symmetric function of

$$\{w(p_2),\cdots,w(p_\lambda)\}.$$

Since $p\rightarrow\{p_2,\cdots,p_\lambda\}$ is a continuous map of P into ${}_{\lambda-1}P$, it follows that the a_i are continuous functions on P. Thus $\tilde{w}$ is continuous on $P\times P$. Clearly $\tilde{w}$ is analytic in q for each fixed p and $\tilde{w}(p,q)\in\mathfrak{A}$ for each fixed p if $w\in\mathfrak{A}$. To show that $\tilde{w}$ is analytic in p, it is enough to show that the elementary symmetric functions of $\{w(p_2),\cdots,w(p_\lambda)\}$ are analytic as functions of p. It is a consequence of Lemma 5 that the elementary symmetric functions of $\{w(p_1),\cdots,w(p_\lambda)\}$ are analytic as functions of p. Now each elementary symmetric function of $\{w(p_2),\cdots,w(p_\lambda)\}$ is a linear combination of an elementary symmetric function of $\{w(p_1),\cdots,w(p_\lambda)\}$ and the product of $w(p_1)=w(p)$ by an elementary symmetric function of $\{w(p_2),\cdots,w(p_\lambda)\}$ of lower order. Thus it follows by induction that the a_i are analytic functions of p.

By Theorem 6,

$$(2\pi i)^{-n}\int_{B_r} g(p)\tilde{w}(p,q)[f_1(p)-f_1(q)]^{-1}\cdots[f_n(p)-f_n(q)]^{-1}df_1(p)\cdots df_n(p)$$
$$=\bar{h}(f(q)),$$

where h is the function on P defined by

$$h(p)=g(p)\tilde{w}(p,q).$$

By Definition 10,

$$\begin{aligned}\bar{h}(z)&=h(p_1)+\cdots+h(p_\lambda)\\&=g(p_1)\tilde{w}(p_1,q)+\cdots+g(p_\lambda)\tilde{w}(p_\lambda,q).\end{aligned}$$

Thus to compute $\bar{h}(f(q))$ we replace $\{p_1,\cdots,p_\lambda\}$ by $\{q_1,\cdots,q_\lambda\}$, obtaining

$$\begin{aligned}\bar{h}(f(q))&=g(q_1)\tilde{w}(q_1,q)+\cdots+g(q_\lambda)\hat{w}(q_\lambda,q)\\&=g(q)\tilde{w}(q,q)=g(q)\hat{w}(q)\end{aligned}$$

since $q_1 = q$ and $\tilde{w}(q_i, q) = 0$ for $2 \leqq i \leqq \lambda$. Since h is analytic on P, $\bar{h}$ is analytic on E^n, so that $h \circ f = g\hat{w}$ is analytic on P. Taking $g = 1$ it follows that $\hat{w}$ is analytic on P.

5. Mappings into higher dimensional spaces. The following lemma continues the study of special analytic polyhedra.

LEMMA 6. *Let P be a special analytic polyhedron in a partially analytic space K defined by functions $f_1, \cdots, f_n$ in $\mathfrak{A}$. Let*

$$P_r = P \cap \{p : |f_i(p)| < r, 1 \leqq i \leqq n\}$$

for $0 < r < 1$. Let $\mathfrak{A}_r$ be the uniform closure of $\mathfrak{A}$ on P_r, so that $\mathfrak{A}_r$ is a Banach algebra in the uniform norm. If σ is any bounded multiplicative linear functional on $\mathfrak{A}_r$, then there exists a point p_0 in P_r such that..

$$\sigma(g) = g(p_0), \text{ all } g \text{ in } \mathfrak{A}_r.$$

If in addition $1 \in \mathfrak{A}_r$ and $\mathfrak{A}_r$ separates points of P_r, there exists a function ϕ in $\mathfrak{A}_r$ which has the value 1 on any open and closed set in P_r and the value 0 on its complement.

Proof. Since σ is bounded, $|\sigma(f_i)| \leqq r$ for $1 \leqq i \leqq n$. Thus

$$z_0 = (\sigma(f_1), \cdots, \sigma(f_n)) \in \bar{E}^n{}_r.$$

We wish to show that there exists p_0 in P_r with $f(p_0) = z_0$ and $\sigma(g) = g(p_0)$ for all g in $\mathfrak{A}$. Assume that this is not the case. Then there exists g_i in $\mathfrak{A}$ with $g_i(p^0{}_i) \neq \sigma(g_i)$ for each $p^0{}_i$ in $\omega(z_0) = \{p^0{}_1, \cdots, p^0{}_\lambda\}$. There therefore exists a linear combination g_0 of $g_1, \cdots, g_\lambda$ such that $g_0(p^0{}_i) \neq \sigma(g_0)$, $1 \leqq i \leqq \lambda$. For each z in E^n and each i with $1 \leqq i \leqq \lambda$ write

$$\delta_i(z) = \sum_{j_1, \cdots, j_i} (-1)^i g_0(p_{j_1}) \cdots g_0(p_{j_i}),$$

where $\{p_1, \cdots, p_\lambda\} = \omega(z)$ and where $j_1, \cdots, j_i$ runs over all combinations of the integers $1, \cdots, \lambda$ taken i at a time. By Lemma 5, δ_i is an analytic function on E^n. If we let $\bar{\delta}_i = \delta_i \circ f$, then clearly

$$(g_0)^\lambda + \sum_{i=1}^{\lambda} \bar{\delta}_i (g_0)^{\lambda - i} = 0$$

identically on P, since

$$[g_0(p)]^\lambda + \sum_{i=1}^{\lambda} \bar{\delta}_i(p) [g_0(p)]^{\lambda - i} = \prod_{i=1}^{\lambda} (g_0(p) - g_0(p_i)) = 0$$

for all p in P. Since δ_i is analytic on E^n, it can be uniformly approximated on $f(P_r) = \bar{E}^n{}_r$ by polynomials F in $z_1, \cdots, z_n$. Therefore $\bar{\delta}_i$ can be uniformly approximated on P_r by polynomials F in $f_1, \cdots, f_n$. Hence $\bar{\delta}_i \in \mathfrak{A}_r$. Since σ is continuous, we have

$$\sigma(\bar{\delta}_i) = \sigma[F(f_1, \cdots, f_n)] = \lim F(\sigma(f_1), \cdots, \sigma(f_n)) \\ = \lim F(z_0) = \delta_i(z_0).$$

Thus

$$0 = [\sigma(g_0)]^\lambda + \sum_{i=1}^{\lambda} [\sigma(\bar{\delta}_i)] [\sigma(g_0)]^{\lambda-i} \\ = [\sigma(g_0)]^\lambda + \sum_{i=1}^{\lambda} [\delta_i(z_0)] [\sigma(g_0)]^{\lambda-i}.$$

Since $\delta_1(z_0), \cdots, \delta_\lambda(z_0)$ are the elementary symmetric functions of $g_0(p^0{}_1), \cdots, g_0(p^0{}_\lambda)$, this implies that $\sigma(g_0) = g_0(p^0{}_i)$ for some i. This contradiction shows that a point p_0 in P_r with the desired property exists. Assume now that $1 \in \mathfrak{A}$. According to what we have just proved, P_r is the maximal ideal space of the Banach algebra $\mathfrak{A}_r$. Therefore according to a theorem of Šilov-Calderon-Arens, (see [1]), the function ϕ exists.

THEOREM 8. *Let K be a weakly holomorphically convex partially analytic space, the maximum of the dimensions of whose structure manifolds is n. Let each n-dimensional structure manifold be open and let their union M_0 be dense in K. Let $\mathfrak{A}$ contain the unit function and separate points of K. For each subset Γ of $\mathfrak{A}$ let each compact component V_0 of each level set V of Γ on K consist of just one point, which is isolated in V. Let $f = (f_1, \cdots, f_n)$, $f_i \in \mathfrak{A}$, be an almost proper map of K into C^n. Let $\{S_k\}$ be a sequence of compact subsets of K, with $\cup S_k = K$ and $S_k \subset$ interior S_{k+1}, each of which has a finite number of components. Let α_i, $1 \leqq i \leqq n$, be positive functions of a real variable x, with $\lim_{x\to\infty} \alpha_i(x) = \infty$. For $r > 0$ let*

$$D_r = \{z : z \in C^n, |z_i| < \alpha_i(r), 1 \leqq i \leqq n\}.$$

For each positive integer k let H_k be the union of those components of $f^{-1}(\bar{D}_k)$ which intersect S_k. Write

$$G_k = [f^{-1}(\bar{D}_k) \cap H_{k+1}] - H_k,$$

for $k \geqq 1$. Write $G_0 = H_1$. For each non-negative integer k let λ_k be any function in $\mathfrak{A}$ and $\epsilon_k < 1$ a positive real number. Then H_k is compact and there exists f_{n+1} in $\mathfrak{A}$ such that

$$|f_{n+1}(p) - \lambda_k(p)| < \epsilon_k, \text{ all } p \text{ in } G_k, \qquad k = 0, 1, 2, \cdots.$$

The map $\bar{f} = f \times f_{n+1}$ of K into C^{n+1} is proper if

$$(\#) \qquad \inf_{p \in G_k} |\lambda_k(p)| \to \infty \text{ as } k \to \infty.$$

If S is a countable subset of M_0 at each point of which rank $f < n$ and rank $\mathfrak{A} = n$, f_{n+1} can in addition be chosen to have the property (*) *rank* $(f_1, \cdots, f_{n+1}) = 1 + \text{rank } f$ *at each point of S. The function f_{n+1} can also be chosen to have the property* (⁑) *of taking distinct values at the points of a given countable subset of K.*

Proof. Let Q be any component of $f^{-1}(D_j)$. Since $\bar{Q}$ is a subset of some component of $f^{-1}(\bar{D}_j)$, $\bar{Q}$ is compact. Thus Q is an analytic polyhedron with frame K defined by multiples of the functions $f_1, \cdots, f_n$. Since each level set of f on Q is closed in $\bar{Q}$, and therefore compact, it follows from the hypotheses of the theorem that such level sets are finite. Therefore Q is a special analytic polyhedron. For k given, choose j so large that $f(S_k) \subset D_j$. Thus each component of S_k is contained in some Q, so that a finite number of such Q cover S_k. The union $\tilde{Q}$ of these Q is an analytic polyhedron. Clearly $H_k \subset \tilde{Q}$, so that H_k is compact.

We construct by induction functions $g_0, g_1, \cdots$ in $\mathfrak{A}$ such that for all $k \geqq 1$

$$|g_k(p)| < \epsilon_k 2^{-(k+1)} \text{ for } p \text{ in } H_k$$

and for all $k \geqq 0$

$$|g_0(p) + \cdots + g_k(p) - \lambda_k(p)| < \tfrac{1}{2}\epsilon_k \text{ for } p \text{ in } G_k.$$

For this purpose there is no loss of generality in assuming that $\epsilon_{k+1} < \epsilon_k$ for all k. Choose $g_0 = \lambda_0$, and assume that $g_0, \cdots, g_{k-1}$ have been chosen with the above properties. Let r be a real number with $k \leqq r < k+1$. From the compactness of H_{k+1} it follows that

$$P^r = H_{k+1} \cap f^{-1}(D_r)$$

is an analytic polyhedron with frame K, defined by multiples of the functions $f_1, \cdots, f_n$. It follows, as above for the analytic polyhedron Q, that P^r is a special analytic polyhedron. By Theorem 5, P^r has only a finite number of components. Also by Theorem 5, applied to P^r, it is easy to see if $k < r < k+1$ that

$$H_{k+1} \cap f^{-1}(\bar{D}_k) = \{p : p \in P^r, |f_i(p)| \leqq \alpha_i(k), 1 \leqq i \leqq n\}$$

is the closure of the set $P^k = f^{-1}(D_k) \cap H_{k+1}$. Since P^k has only a finite number of components, the set

$$G_k \cup H_k = f^{-1}(\bar{D}_k) \cap H_{k+1}$$

has only a finite number of components. By the definition of H_k, H_k is the union of certain components of $G_k \cup H_k$; therefore G_k is the union of the remaining components of $G_k \cup H_k$. Thus G_k and H_k are disjoint closed sets.

Since $G_k \cup H_k$ is the intersection of the nested compact sets $\overline{P^r}$, $k < r < k+1$, there therefore exists a value of r in the range such that the finite number of components of $G_k \cup H_k$ all belong to separate components of $\overline{P^r}$. Then G_k belongs to an open and closed set W in $\overline{P^r}$ and H_k belongs to $\overline{P^r} - W$. It follows from Lemma 6 that there exists a function τ in $\mathfrak{A}$ which is arbitrarily near to 0 on H_k and to 1 on G_k. Write

$$g_k = -\tau[g_0 + \cdots + g_{k-1} - \lambda_k].$$

It is then clear that g_k has the desired properties if τ is near enough to 0 and 1 on H_k and G_k respectively.

Define

$$f_{n+1} = \sum_{k=0}^{\infty} g_k.$$

This series converges uniformly on H_k since for $j \geqq k$

$$| g_j(p) | < \epsilon_j 2^{-(j+1)} \text{ for } p \in H_k \subset H_j.$$

Now if Δ is any compact subset of K, there exists j with $\Delta \subset S_j$. If $k > j$ is chosen so large that $f(S_j) \subset D_k$, it follows that $\Delta \subset S_j \subset H_k$. Therefore the series for f_{n+1} is well-defined and lies in $\mathfrak{A}$. For p in G_k we have

$$| \lambda_k(p) - f_{n+1}(p) | \leqq | \lambda_k(p) - \sum_{j=0}^{k} g_j(p) | + \sum_{j=k+1}^{\infty} | g_j(p) |$$
$$< \tfrac{1}{2}\epsilon_k + \sum_{j=k+1}^{\infty} \epsilon_k 2^{-j} \leqq \epsilon_k.$$

Thus the function f_{n+1} satisfies the required inequalities. An obvious modification of the proof yields a function f_{n+1} which in addition has properties $(*)$ and $(\overset{*}{\#})$.

It remains to show that $f \times f_{n+1} = \bar{f}$ is proper if the condition $(\#)$ is satisfied. Consider p in $\bar{f}^{-1}(F_k)$, where $F_k = D_k \times \{z \colon z \in C^1, | z | < k\}$. Let j be the smallest integer $\geqq k$ such that $p \in H_j$. If $j > k$, then p is in G_{j-1}. Therefore

$$k > | f_{n+1}(p) | > | \lambda_{j-1}(p) | - \epsilon_{j-1}$$

It follows from condition $(\#)$ that this can happen for only a finite number of values of j. Therefore $\bar{f}^{-1}(F_k)$ is contained in the union of H_k and such H_j. Since H_j and H_k are compact, this implies that $\bar{f}$ is proper, as was to be proved.

The hypothesis in the last theorem, and also in the following theorem, that compact components V_0 of V consist of just one point,, which is isolated in V, is in fact unnecessary if K is a complex space. This can be seen from results of Stein [11], which states that if f is an analytic mapping of a complex space K having the property that the components of the level sets of f on K are compact then it is possible to introduce an analytic structure into the class $\bar{K}$ of such components in such a way that the natural map of K into $\bar{K}$ is analytic. However, we will not pursue this question here.

THEOREM 9. *Let K be a weakly holomorphically convex partially analytic space, the maximum of the dimensions of whose structure manifolds is n. Let each n-dimensional structure manifold be open and let their union M_0 be dense in K. Let $\mathfrak{A}$ contain the unit function and separate points of K. For each subset Γ of $\mathfrak{A}$ let each compact component V_0 of each level set of V on K consist of just one point, which is isolated in V. Let K be the union of a sequence S_k of compact sets, each having a finite number of components, with $S_k \subset$ interior S_{k+1}. Let M be a particular n-dimensional structure manifold of K, such that $\mathfrak{A}$ has rank n at each point of M. Let G be the set of functions $(f_1, \cdots, f_{2n+1})$ in ${}^{2n+1}\mathfrak{A}$ such that*

(i) *$f = (f_1, \cdots, f_n)$ is almost proper,*

(ii) *$\bar{f} = (f_1, \cdots, f_{n+1})$ is proper,*

(iii) *the rank of $(f_1, \cdots, f_{2n})$ at each point of M is n,*

(iv) *the functions $(f_1, \cdots, f_{2n+1})$ separate points of M.*

Then G is dense in ${}^{2n+1}\mathfrak{A}$.

Proof. By Theorem 4, the elements f in ${}^{n}\mathfrak{A}$ which are almost proper are dense. Fix such an element f. If V is a level set of f, each component V_0 of V is compact because f is almost proper. It follows from the hypothesis of the theorem that V_0 consists of one point, which is isolated in V. Therefore V is countable, so that all level sets of f are countable. For $1 \leqq i \leqq n$ let A^0_i consist of all points in M at which rank $f < i$. Each of these sets is analytic in M and $A^0_i \subset A^0_{i+1}$. Clearly

$$\dim A^0_n < \dim M = n,$$

since f, whose level sets are countable, must have rank n at some point of M. We now show inductively, starting with $i = n$ and working backward, that $\dim A^0_i < i$. Assume therefore that $\dim A^0_{i+1} < i + 1$. Let the analytic set A^0_{i+1} be written as the union of submanifolds $\{N^{i+1}_\gamma\}$ of M, and let $\{N^{i+1}_\beta\}$ consist of those N^{i+1}_γ of dimension i. To show $\dim A^0_i < i$, it will be sufficient to show that A^0_i does not contain any of the N^{i+1}_β. For if this is the case the inclusion $A^i_0 \subset A^0_{i+1}$ implies that A^0_i is contained in the union of certain proper analytic subsets of the $N^{i+1}{}_\beta$ and of the $N^{i+1}{}_\gamma$ of dimension less than i. so that $\dim A^0{}_i < i$. To see that $N^{i+1}{}_\beta \not\subset A^0{}_i$, note that f has rank i at some point of $N^{i+1}{}_\beta$, since its level sets are countable and $\dim N^{i+1}{}_\beta = i$. This completes the proof that $\dim A^0{}_i < i$.

Let S be a countable dense set in M. For each $N^i{}_\beta$, $1 \leqq i \leqq n$, choose a point $p^i{}_\beta$ in $N^i{}_\beta$ at which the rank of f is at least $i-1$. Let H be the set of all f_{n+1} in $\mathfrak{A}$ such that $\bar{f} = f \times f_{n+1}$ is proper, such that $\bar{f}$ has rank i on M at the point $p^i{}_\beta$ for each i and β, and such that f_{n+1} takes distinct values at the points of the set $f^{-1}(S)$. By Theorem 8, there exists f_{n+1} in H such that

$$|f_{n+1}(p) - \lambda(p)| < \epsilon$$

for all p in $G_0 = H_1$ where H_1 is defined as in Theorem 8, where λ is any function in $\mathfrak{A}$, and where $\epsilon > 0$. Since by an appropriate choice of the sequence $\{S_k\}$ and the functions α_i of Theorem 8 the set H_1 can be made to contain any compact subset of K, it follows that H is dense in $\mathfrak{A}$.

We now choose the functions $f_{n+2}, \cdots, f_{2n+1}$ by induction. Assuming that $f_{n+1}, \cdots, f_{n+k}$ have been chosen, let $A^k{}_i$, $1 \leqq i \leqq n$, consist of all points in M at which $f_1, \cdots, f_{n+k}$ have rank less than i. Clearly each $A^k{}_i$ is an analytic subset of M. Let B_k consist of all points in $M - A^k{}_n$ which are identified with some other point of M by the functions $f_1, \cdots, f_{n+k}$. Since $\bar{f}$ is proper, the points in K which are identified with a given point p in B_k by the functions $f_1, \cdots, f_{n+k}$ form a compact set L. By the hypothesis of the theorem it follows that L is finite. Let $p = p_1, \cdots, p_j$ be the points of $M \cap L$. Let ϵ be a small positive number and write

$$g_i = \epsilon^{-1}(f_i - f_i(p)), \qquad 1 \leqq i \leqq n.$$

Since f is almost proper $g = (g_1, \cdots, g_n)$ is almost proper. Therefore each component of $g^{-1}(E^n)$ is an analytic polyhedron defined by g with frame K. Let P_m be that component of $g^{-1}(E^n)$ which contains p_m, $1 \leqq m \leqq j$. For a fixed m the intersection I_m of the P_m, taken for all values of ϵ, is clearly a subset of the countable discrete set $f^{-1}(f(p))$. Since I_m is also the intersection of the P_m, which are nested connected compact sets, it follows that I_m is connected. Hence $I_m = \{p_m\}$. It follows that ϵ can be chosen so small that $P_1, \cdots, P_j$ are disjoint subsets of M. We can also choose ϵ so small that $(f_1, \cdots, f_{n+k})$ is one-to-one on P_1, since $p_1 = p \in M - A^k{}_n$. Write

$$h_i = \epsilon^{-1}(f_i - f_i(p)), \qquad 1 \leqq i \leqq n+k,$$

$h = (h_1, \cdots, h_{n+k})$. It follows by an argument similar to the one just used that there exists a neighborhood $U \subset P_1$ of p such that

$$U \cap B_k = U \cap h^{-1}(P_2 \cup \cdots \cup P_j)).$$

Now h maps P_m properly into $E^n \times C^k$, since P_m is an analytic polyhedron defined by $g = (h_1, \cdots, h_n)$. Let $W_m = h(P_m)$. Since h is proper on P_m, it follows from a standard result ([9], Satz 23) that W_m is an analytic subset of $E^n \times C^k$. Thus $W = W_2 \cup \cdots \cup W_j$ is analytic. Thus $U \cap h^{-1}(W) = U \cap B_k$ is an analytic subset of U. Since p was any point in B_k, it follows that B_k is locally analytic.

We choose the functions $f_{n+2}, \cdots, f_{2n+1}$ by induction to be arbitrarily close to given functions in $\mathfrak{A}$ on a given compact subset of K and to have the properties

$$\dim A^k{}_i < \max\{0, i - k\},$$

$$\dim B_k < n - k + 1.$$

We first check that the function f_{n+1} already chosen has these properties. Since $\bar{f}$ has rank i on M at $p^i{}_\beta$, it follows that $A^1{}_i$ intersects $N^i{}_\beta$ in a proper subset, which therefore has dimension at most i $-$ 2. Since $A^1{}_i \subset A^0{}_i$, it then follows as above that $\dim A^1{}_i \leqq i - 2$. Let p be any point in $S - A^1{}_n$. By the choice of f_{n+1} we see that $p \notin B_1$. Thus B_1 is a proper analytic subset of the manifold $M - A^1{}_n$; it follows that $\dim B_1 < n$.

Assume now that $f_1, \cdots, f_{n+k}$ have been chosen so that the above dimension inequalities are true. Write

$$A^k{}_i = \bigcup_\beta N^\beta{}_{ik},$$

a countable union of submanifolds of M. Write

$$B_k = \bigcup_\beta J_\beta,$$

a countable union of submanifolds of M. Now if $i - k > 0$, consider $N^\beta{}_{ik}$ of dimension $i - k - 1$, the maximum possible dimension by the induction hypothesis. Since $N^\beta{}_{ik} \not\subset A^k{}_{i-1}$, $(f_1, \cdots, f_{n+k})$ have rank at least $i - 1$ at some point $p^\beta{}_{ik}$ of $N^\beta{}_{ik}$. Thus f_{n+k+1} can be chosen to be arbitrarily close to a given function in $\mathfrak{A}$ on a given compact subset of K and to have the property that $f_1, \cdots, f_{n+k+1}$ has rank i at $p^\beta{}_{ik}$ for each $p^\beta{}_{ik}$. It follows then that

$$\dim A^{k+1}{}_i < \max\{0, i - k - 1\}.$$

The function f_{n+k+1} can be chosen to have the additional property that each J_β contains some point p not identified by f_{n+k+1} with any of the points which $f_1, \cdots, f_{n+k}$ identify with p. Thus p is not in B_{k+1}, so that B_{k+1} intersects J_β in a set of dimension at most $(\dim J_\beta) - 1 \leqq (\dim B_k) - 1 < n - k$. Since

$$B_{k+1} \subset B_k \cup A^k{}_n \subset \cup J_\beta \cup A^k{}_n,$$

it follows that

$$\dim B_{k+1} \leqq \max\{\dim A^k{}_n, \dim B_{k+1} \cap J_\beta\} < n - k = n - (k+1) + 1.$$

Thus the functions $f_1, \cdots, f_{2n+1}$ with the desired properties are dense in ${}^{2n+1}\mathfrak{A}$. Now (iii) follows from the fact that

$$\dim A^n{}_n < \max\{0, n - n\} = 0,$$

so that $A^n{}_n$ is void. Finally, (iv) follows from the fact that $A^{n+1}{}_n \subset A^n{}_n$ is void and that

$$\dim B_{n+1} < n - (n+1) + 1 = 0, \text{ so that } B_{n+1} \text{ is void.}$$

This completes the proof.

UNIVERSITY OF CALIFORNIA, BERKELEY.

REFERENCES.

[1] R. Arens and A. P. Calderon, "Analytic functions of several Banach algebra elements," *Annals of Mathematics*, vol. 62 (1955), pp. 204-216.

[2] H. Behnke and K. Stein, "Modification komplexer Mannigfaltigkeiten und Riemannscher Gebiete," *Mathematische Annalen*, vol. 124 (1955), pp. 1-16.

[3] S. Bergmann, "Über eine in gewissen Bereichen mit Maximumflache gültige Integral darstellung der Funktionen zweier komplexer Variabler," *Mathematische Zeitschrift*, vol. 39 (1934), pp. 76-94.

[4] H. Cartan, *Séminaire Ecole Normale Supérieure*, 1951-1952.

[5] ———, *Séminaire Ecole Normale Supérieure*, 1953-1954.

[6] H. Grauert, "Characterzierung der holomorphvolständigen komplexen Räume," *Mathematische Annalen*, vol. 129 (1955), pp. 233-259.

[7] W. Hurewicz and H. Wallman, *Dimension theory*, Princeton, 1948.

[8] R. Remmert, "Sur les espaces analytiques holomorphiquement separables et holomorphiquement convexes," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, Paris, vol. 243 (1956), pp. 118-121.

[9] ———, "Holomorphe und meromorphe Abbildungen komplexer Räume," *Mathematische Annalen*, vol. 133 (1957), pp. 328-370.

[10] H. Rossi, *Analytic spaces*, U. S. Air Force technical report, Princeton University, 1960.

[11] K. Stein, "Analytische Zerlegungen komplexer Räume," *Mathematische Annalen*, vol. 132 (1956), pp. 63-93.

[12] ——— and R. Remmert, "Über die wesentlichen Singularitäten analytischer Mengen," *ibid.*, vol. 126 (1953), pp. 263-306.

[13] A. Weil, "L'intégrale de Cauchy et les fonctions de plusieurs variables," *ibid.*, vol. 111 (1935), pp. 178-182.

PARTITIONS IN CERTAIN ARITHMETIC PROGRESSIONS.*

By Shô Iseki.

Introduction. Let $\mathfrak{a} = \{a_1, a_2, \cdots, a_\nu\}$ be a set of ν distinct integers satisfying $0 < a_j < M$, $(a_j, M) = 1$ $(j = 1, 2, \cdots, \nu)$, where M is an integer $\geqq 2$. Such a set $\mathfrak{a}$ will be called *symmetric,* if with a also $M - a$ belongs to $\mathfrak{a}$.

For any given nonnegative integer n, one may consider partitions[1] of n into positive summands whose least positive residues $(\operatorname{mod} M)$ belong to $\mathfrak{a}$, or in other words, partitions of n into numbers of the form $Ml + a_j$ $(l = 0, 1, 2, \cdots; j = 1, 2, \cdots, \nu)$. In case M is an odd prime, this partition problem was treated by E. Grosswald [2], who obtained an asymptotic formula for the partition function.

When $\mathfrak{a}$ is symmetric, the special case $\mathfrak{a} = \{a, M - a\}$ $(M \geqq 3)$ may be regarded as fundamental; in this case the corresponding partition function $p(n; a, M)$ has been fully discussed in [5].

In the present paper we shall be concerned with another interesting case of symmetric sets. Namely we shall treat the partition function associated with a symmetric set $\mathfrak{a}$ consisting of all integers a for which $0 < a < M$, $(a, M) = 1$; or more simply, the number of partitions of n into those summands which are positive and prime to M. This partition function will be denoted by $p_M(n)$. Applying the method developed in [5] we shall find a suitable transformation formula for the generating function of $p_M(n)$ and represent $p_M(n)$ exactly as a convergent infinite series. The same method would also be valid for general symmetric sets, though we shall not go so far in this research.

In case $M = 3$ or 6, our partition function $p_M(n)$ is identical with $p(n; 1, M)$ mentioned above, and in case $M = 2$ it reduces to $p(n; 1, 4)$ (cf. L. K. Hua [4], I. Niven [8]). M. Haberzetle [3] has treated the case where M is a product of two different primes under the restriction that $\phi(M) \equiv 0$ (mod 24), $\phi(M)$ being the Euler function. This restriction she imposed

---

* Received September 7, 1960.

[1] By 'the number of partitions of n' we mean the number of solutions of

$$n = n_1 s_1 + n_2 s_2 + \cdots$$

in nonnegative integers $n_1, n_2, \cdots$, where $s_1, s_2, \cdots$ are the given (positive) summands. This implies, in particular, that when $n = 0$ the partition number is 1.

on M in order to avoid difficulties arising from the estimation of certain exponential sums which occur in the analysis.

The present paper will deal with $p_M(n)$ for general values of M, covering all the previously known results which were obtained in particular cases. We may assume, without loss of generality, that M is a square-free number. In Section 1 we shall develop a transformation theory for the generating function $F_M(x)$ of the partition function $p_M(n)$; the result is possibly of some interest in itself, apart from its application to the partition theory. We shall show, among others, that $F_M(x)$ is transformed into $F_M(x')$ or into $F_M^{-1}(x')$ $(=1/F_M(x'))$ by taking an appropriate new variable x'. In their treatments of the special cases, Niven [8] and Haberzetle [3] have utilized the theory of the Dedekind modular function to derive the transformation formula for $F_M(x)$. Their method, however, seems to be unfeasible in the general case. For our method, on the other hand, it is unnecessary to make any use of the theory of modular functions. In Section 2, we shall study a certain sum of complicated roots of unity which will be needed in the analysis. This sum can be reduced to a generalized Kloosterman sum and consequently a satisfactory estimate for the sum will be obtained. In both Sections 1 and 2, frequent quotations will be made from [5] so as to establish the desired results. In Section 3 we shall obtain a series expansion for $p_M(n)$ in terms of Bessel functions, by using the method of Rademacher [9]. This expansion is valid for all nonnegative integers n, except that, in case $\phi(M)\equiv 0 \pmod{24}$ and the Möbius function $\mu(M)$ is equal to $+1$, we have to assume that $n\neq\phi(M)/24$. The final section is devoted to derivation of asymptotic formulae for $p_M(n)$ for large values of n. The method in this section will be quite analogous to that of [5, § 4]. We shall give an asymptotic formula in terms of elementary functions of n as well as a more precise formula involving a Bessel function.

1. Transformation theory for the generating function. The generating function $F_M(x)$ of the partition function $p_M(n)$ is given by

$$F_M(x)=\sum_{n=0}^{\infty}p_M(n)x^n=\prod_{\substack{l=1\\(l,M)=1}}^{\infty}(1-x^l)^{-1}\qquad(|x|<1).$$

Our subject in this section is to establish a transformation formula for $F_M(x)$ which will exhibit the behavior of $F_M(x)$ in the neighborhood of its singularity at each rational point of the unit circle. To this effect, we put

$$x=\exp(2\pi ih/k-2\pi z/k),$$

where h, k are coprime integers $(k \geqq 1)$, and z is a complex variable with $\Re(z) > 0$. Further, let

$$K = \text{L. C. M. of } k, M; \qquad D = \text{G. C. D. of } k, M,$$

and put $k = k_1 D$, $M = m_1 D$. Then we have $(m_1, k_1) = 1$ and $(m_1, D) = 1$ (the latter follows from the stipulation that M is square-free), so that also $(m_1, k) = 1$. Take, then, an integer H to be any fixed solution of the congruence

$$(1.1) \qquad m_1 h H \equiv -1 \pmod{k},$$

which is solvable on account of $(h, k) = (m_1, k) = 1$; and set

$$x' = \exp(2\pi i H/k - 2\pi/Kz).$$

We are now in a position to state our transformation theorem.

THEOREM 1. *We have*

$$(1.2) \qquad \begin{aligned} F_M(x) = {} & \tau(M, D)\Omega_M(h, k) \\ & \cdot \exp\{(\pi\phi(M)/12k)(\mu(D)/m_1 z - \mu(M) z)\} F_M^{\epsilon}(x'). \end{aligned}$$

Here

$$(1.3) \qquad \tau(M, D) = \begin{cases} M^{-\frac{1}{2}}, \textit{ if } M \textit{ is a prime and } D = 1, \\ 1, \quad \textit{otherwise}; \end{cases}$$

$\phi(t)$ *and* $\mu(t)$ *are, respectively, the Euler and the Möbius functions*; $\epsilon = \mu(m_1)$, *and* $\Omega_M(h, k)$ *is a root of unity defined by*

$$(1.4) \qquad \Omega_M(h, k) = \exp\{\pi i \Sigma_M(h, k)\}$$

with the notation

$$(1.5) \qquad \Sigma_M(h, k) = \sum_{\substack{0<\lambda<K \\ (\lambda, M)=1}} ((\lambda/K))((h\lambda/k)) \qquad (M \geqq 3),$$

$$(1.6) \qquad \Sigma_2(h, k) = \begin{cases} \displaystyle\sum_{\substack{0<\lambda<k \\ (\lambda,2)=1}} ((\lambda/k))((h\lambda/k)), \quad \textit{if } 4 \mid k, \\ \displaystyle\sum_{\substack{0<\lambda<2k \\ (\lambda,2)=1}} ((\lambda/2k))((h\lambda/k)), \quad \textit{if } 2 \mid k \textit{ and } 4 \nmid k, \\ \displaystyle\sum_{\substack{0<\lambda<4k \\ (\lambda,2)=1}} ((\lambda/4k))((h\lambda/k)), \textit{ if } 2 \nmid k, \end{cases}$$

where

$$(1.7) \qquad ((t)) = \begin{cases} 0, \textit{ if } t \textit{ is an integer}, \\ t - [t] - \frac{1}{2}, \textit{ otherwise}, \end{cases}$$

$[t]$ *denoting the greatest integer not exceeding* t.

To prove Theorem 1, we require the following lemma.

Lemma 1. *Let N be a positive integer, and $\mu(t)$ the Möbius function.*

1) *If $f(t)$ is any function defined for $0 < t \leqq 1$, then*

$$\sum_{\substack{1\leqq r\leqq N\\(r,N)=1}} f(r/N) = \sum_{d|N}\mu(N/d)\sum_{1\leqq r\leqq d} f(r/d).$$

2) *If $f(t)$ is any function defined for $0 < t \leqq 1$ and $f(t) \neq 0$, then*

$$\prod_{\substack{1\leqq r\leqq N\\(r,N)=1}} f(r/N) = \prod_{d|N}\{\prod_{1\leqq r\leqq d} f(r/d)\}^{\mu(N/d)}.$$

3) *If $g(t)$ is an arithmetical function for which $\prod_{l=1}^{\infty} g(l)$ is absolutely convergent, then*

$$\prod_{\substack{l=1\\(l,N)=1}}^{\infty} g(l) = \prod_{n=1}^{\infty}\prod_{d|N}\{g(nd)\}^{\mu(d)}.$$

Proof.

1) We apply the Möbius inversion formula:

$$\sum_{d|N} F(d) = G(N) \textit{ implies } F(N) = \sum_{d|N}\mu(N/d)G(d)$$

to the obvious identity

$$\sum_{d|N}\sum_{\substack{1\leqq r\leqq d\\(r,d)=1}} f(r/d) = \sum_{1\leqq r\leqq N} f(r/N),$$

and the result follows.

2) The proof is similar to that of 1) and may be omitted.

3) Since

$$\prod_{\substack{l=1\\(l,N)=1}}^{\infty} g(l) = \prod_{\substack{1\leqq r\leqq N\\(r,N)=1}}\prod_{s=0}^{\infty} g(r+sN) = \prod_{\substack{1\leqq r\leqq N\\(r,N)=1}}\prod_{s=0}^{\infty} g(N(r/N+s)),$$

we can apply 2) with $f(t) = \prod_{s=0}^{\infty} g(N(t+s))$. The right member of the identity in 2) then becomes

$$\prod_{d|N}\{\prod_{1\leqq r\leqq d}\prod_{s=0}^{\infty} g(N(r/d+s))\}^{\mu(N/d)}$$
$$=\prod_{d|N}\{\prod_{1\leqq r\leqq d}\prod_{s=0}^{\infty} g((N/d)(r+sd))\}^{\mu(N/d)} = \prod_{d|N}\{\prod_{n=1}^{\infty} g((N/d)n)\}^{\mu(N/d)}$$
$$=\prod_{n=1}^{\infty}\prod_{d|N}\{g((N/d)n)\}^{\mu(N/d)}.$$

The required result now follows on replacing d by N/d.

In what follows in this section, we shall sometimes say that two integers n_1, n_2 are *complementary with respect to* N to mean that they satisfy the relation $n_1 + n_2 = N$ for a fixed positive integer N.

We now proceed to the proof of Theorem 1.

Let us treat first the case $M \geqq 3$. We begin by introducing $\frac{1}{2}\phi(M)$ $(=\kappa)$ integers $a_1, a_2, \cdots, a_\kappa$ defined as follows:

Case 1). $D = 1$ *or* 2. Let $a_1, a_2, \cdots, a_\kappa$ be the set of all distinct integers a for which $0 < a < M/2$, $(a, M) = 1$.

Case 2). $D \geqq 3$. Take an integer b of the interval $0 < b < D/2$ with $(b, D) = 1$, and another integer c of the interval $0 \leqq c < m_1$ with $(c, m_1) = 1$. Define, then, an integer a by

$$0 < a < M, \quad ha \equiv b \pmod{D}, \quad a \equiv c \pmod{m_1}. \tag{1.8}$$

Since $(h, D) = (D, m_1) = 1$ and $Dm_1 = M$, it is plain that (1.8) yields a unique a for any set of h, b, c. This being so, we keep h fixed and let b, c range over their values, so that we have in all $\frac{1}{2}\phi(D) \cdot \phi(m_1) = \frac{1}{2}\phi(M)$ such integers a. Let these a's be $a_1, a_2, \cdots, a_\kappa$. We then see that these integers are distinct and prime to M and pairwise incomplementary with respect to M. (If, for example, a_1, a_2 were complementary with respect to M, then we should have $b_1 + b_2 \equiv 0 \pmod{D}$, where b_1, b_2 are the values of b which correspond to a_1, a_2 respectively. But this is impossible since $0 < b_1 < D/2$, $0 < b_2 < D/2$).

From the above definition, it follows that in both Cases 1) and 2), all the integers a satisfying $0 < a < M$, $(a, M) = 1$ are just given by $a_1, a_2, \cdots, a_\kappa$, $M - a_1, M - a_2, \cdots, M - a_\kappa$. Accordingly, our generating function $F_M(x)$ can be expressed in the form

$$F_M(x) = \prod_{a \in \mathfrak{A}} F(x; a, M), \qquad \mathfrak{A} = \{a_1, a_2, \cdots, a_\kappa\}, \tag{1.9}$$

where

$$F(x; a, M) = \prod_{m=0}^{\infty} (1 - x^{mM+a})^{-1} (1 - x^{mM+M-a})^{-1}.$$

Some properties of the function $F(x; a, M)$ have been studied in [5] and [6]. We quote here the transformation theory for $F(x; a, M)$ from [5, § 1] and [6, Theorem 2]:[2]

Choose any fixed pair of integers γ, δ such that $\gamma k_1 - \delta m_1 = 1$. Define then an integer H as any fixed solution of the congruence $hH \equiv \delta \pmod{k}$.

---

[2] In what follows, the letters M, h, k, z, K, D, k_1, m_1 have the same meanings as before, though M is not necessarily restricted to be square-free in [5] and [6].

Let

$$x = \exp(2\pi ih/k - 2\pi z/k), \qquad x' = \exp(2\pi iH/k - 2\pi/Kz).$$

Also define

$$a = \text{an integer of the interval } 0 < a < M \text{ with } (a, M) = 1,$$
$$\rho_a = \exp(-2\pi ia\gamma/M),$$

(1.10) $b = b(a) = ha - D[ha/D]$ (note that $ha \equiv b \pmod D$, $0 \leqq b < D$),

(1.11) $$A = 6a^2 - 6Ma + M^2, \qquad B = 6b^2 - 6Db + D^2,$$

(1.12) $$\omega_a(h, k) = \exp\{2\pi i\sigma_a(h, k)\}, \quad \sigma_a(h, k) = \sum_{\mu_a} ((\mu_a/K))((h\mu_a/k))$$
$$(\mu_a = a, M + a, 2M + a, \cdots, (k_1 - 1)M + a),$$

(1.13) $$F(x'; b, D, \rho_a) = \prod_{m=0}^{\infty} (1 - \rho_a x'^{mD+b})^{-1}(1 - \rho_a^{-1} x'^{mD+D-b})^{-1} \quad (D > 1).$$

In the case $D = 1$, we define an integer ξ_a by

(1.14) $$\xi_a k \equiv a \pmod M \quad (0 < \xi_a < M);$$

then we have $\rho_a = \exp(-2\pi i\xi_a/M)$. We note that for $D = 1$, H is also determined by the congruence $MhH \equiv -1 \pmod k$, which is coincident with the special case $D = 1$ of (1.1).

With the above notations we have the tranformation formulae:

$$F(x; a, M) = \omega_a(h, k)\exp\{(\pi/6Mk)(B/z - Az)\}F(x'; b, D, \rho_a)$$

for $D > 1$, and

$$F(x; a, M) = \tfrac{1}{2}\csc(\pi\xi_a/M)\omega_a(h, k)\exp\{(\pi/6Mk)(B/z - Az)\}$$
$$\cdot \prod_{m=1}^{\infty} (1 - \rho_a x'^m)^{-1}(1 - \rho_a^{-1} x'^m)^{-1}$$

for $D = 1$.[3]

Consequently we obtain, by (1.9),

(1.15) $$F_M(x) = \omega^*(h, k)\exp\{(\pi/6Mk)(B^*/z - A^*z)\} \prod_{a \in \mathfrak{A}} F(x'; b, D, \rho_a)$$

for $D > 1$,[4] and

(1.16) $$F_M(x) = \prod_{a \in \mathfrak{A}} \tfrac{1}{2}\csc(\pi\xi_a/M) \cdot \omega^*(h, k)\exp\{(\pi/6Mk)(B^*/z - A^*z)\}$$
$$\cdot \prod_{a \in \mathfrak{A}} \prod_{m=1}^{\infty} (1 - \rho_a x'^m)^{-1}(1 - \rho_a^{-1} x'^m)^{-1}$$

---

[3] When $D = 1$, the actual value of B is 1.

[4] We remark that in the case $D \geqq 3$, the letter b means the same thing in (1.15) as in (1.8) by virtue of (1.10).

for $D = 1$, where

$$\omega^*(h,k) = \prod_{a\in\mathfrak{A}} \omega_a(h,k), \qquad A^* = \sum_{a\in\mathfrak{A}} A, \qquad B^* = \sum_{a\in\mathfrak{A}} B. \tag{1.17}$$

Let us now calculate the values of A^* and B^*. It is clear from (1.11) that A is invariant under the transformation $a \to M - a$, and therefore

$$A^* = \tfrac{1}{2} \sum_{\substack{0<a<M\\(a,M)=1}} A = \tfrac{1}{2} \sum_{\substack{0<a<M\\(a,M)=1}} (6a^2 - 6Ma + M^2)$$
$$= \tfrac{1}{2}M^2 \sum_{\substack{0<a<M\\(a,M)=1}} \{6(a/M)^2 - 6a/M + 1\}.$$

Furthermore, by Lemma 1.1), this becomes

$$\tfrac{1}{2}M^2 \sum_{d\mid M} \mu(M/d) \sum_{1\leqq a\leqq d} \{6(a/d)^2 - 6a/d + 1\} = \tfrac{1}{2}M^2 \sum_{d\mid M} \mu(M/d)/d$$
$$= \tfrac{1}{2}M^2 \sum_{d\mid M} \mu(d)\, d/M = \tfrac{1}{2}M \sum_{d\mid M} \mu(d)\, d = \tfrac{1}{2}M\mu(M)\phi(M).$$

Thus

$$A^* = \tfrac{1}{2}M\mu(M)\phi(M). \tag{1.18}$$

Next, to evaluate B^* for $D \geqq 3$, we take into account the relation between a and b which is shown in (1.8). We obtain

$$B^* = \tfrac{1}{2}\phi(m_1) \sum_{\substack{0<b<D\\(b,D)=1}} (6b^2 - 6Db + D^2) = \tfrac{1}{2}\phi(m_1) D\mu(D)\phi(D)$$
$$= \tfrac{1}{2}D\mu(D)\phi(M).$$

When $D = 2$, we have $b = 1$ for all a, and hence

$$B^* = \tfrac{1}{2}\phi(M)(6 - 6\cdot 2 + 2^2) = \tfrac{1}{2}\, 2\mu(2)\phi(M);$$

while, when $D = 1$, we have $b = 0$ for all a, and so

$$B^* = \tfrac{1}{2}\phi(M).$$

Consequently, for all values of D, we have

$$B^* = \tfrac{1}{2}D\mu(D)\phi(M). \tag{1.19}$$

Now by (1.12) and (1.17) we get

$$\omega^*(h,k) = \exp\{2\pi i\sigma^*(h,k)\}, \qquad \sigma^*(h,k) = \sum_{a\in\mathfrak{A}} \sigma_a(h,k), \tag{1.20}$$
$$\sigma_a(h,k) = \sum_{\mu_a} ((\mu_a/K))((h\mu_a/k))$$
$$(\mu_a = a, M+a, 2M+a, \cdots, (k_1-1)M+a).$$

Here $((t))$ is an odd function of t and has period 1, as is seen from (1.7), so that

$$\sigma_a(h,k)=\sum_{\mu_a}(((K-\mu_a)/K))((h(K-\mu_a)/k))=\sum_{\nu_a}((\nu_a/K))((h\nu_a/k))$$
$$(K-\mu_a=\nu_a\,;\,\nu_a=M-a,2M-a,\cdots,k_1M-a).$$

Therefore

$$2\sigma^*(h,k)=\sum_{a\in\mathfrak{A}}\sum_{\mu_a}((\mu_a/K))((h\mu_a/k))+\sum_{a\in\mathfrak{A}}\sum_{\nu_a}((\nu_a/K))((h\nu_a/k))$$
$$=\sum_{\substack{0<\lambda<K\\(\lambda,M)=1}}((\lambda/K))((h\lambda/k))=\Sigma_M(h,k)$$

by (1.5). It then follows from (1.20) that

$$\omega^*(h,k)=\exp\{\pi i\Sigma_M(h,k)\},$$

and hence, by (1.4),

$$\omega^*(h,k)=\Omega_M(h,k). \tag{1.21}$$

Our argument is now split into three cases according as $D\geqq 3$, $D=2$, or $D=1$.

Case i). $D\geqq 3$. By (1.13), we have

$$\prod_{a\in\mathfrak{A}}F(x';b,D,\rho_a)=\prod_{m=0}^{\infty}\prod_{a\in\mathfrak{A}}(1-\rho_a x'^{mD+b})^{-1}(1-\rho_a^{-1}x'^{mD+D-b})^{-1}, \tag{1.22}$$

in which the left member has appeared in (1.15). Here $\rho_a=\exp(-2\pi ia\gamma/M)$, and γ is defined by $\gamma k_1\equiv 1 \pmod{m_1}$. Let us now employ that γ which satisfies the additional condition $\gamma\equiv 0 \pmod D$. Putting $\gamma=\gamma_1 D$, we have $\rho_a=\exp(-2\pi ia\gamma_1/m_1)$, where $(\gamma_1,m_1)=1$. We note, in passing, that γ_1, δ are then defined by $\gamma_1 k-\delta m_1=1$ and H by $m_1hH\equiv -1 \pmod k$, and that this congruence coincides with (1.1).

Now, remembering that the integers $a_1,a_2,\cdots,a_K$ are constructed by means of the congruences $ha\equiv b \pmod D$ $(0<b<D/2,\ (b,D)=1)$, $a\equiv c \pmod{m_1}$ $(0\leqq c<m_1,\ (c,m_1)=1)$ (see (1.8)) and observing that $\rho_a=\exp(-2\pi ic\gamma_1/m_1)$, we obtain

$$\begin{aligned}&\prod_{a\in\mathfrak{A}}(1-\rho_a x'^{mD+b})^{-1}(1-\rho_a^{-1}x'^{mD+D-b})^{-1}\\ &\quad=\prod_{\substack{0<b<D/2\\(b,D)=1}}\prod_{\substack{0\leqq c<m_1\\(c,m_1)=1}}(1-\exp(-2\pi ic\gamma_1/m_1)x'^{mD+b})^{-1}\\ &\qquad\cdot(1-\exp(2\pi ic\gamma_1/m_1)x'^{mD+D-b})^{-1}.\end{aligned} \tag{1.23}$$

Here, since $(\gamma_1,m_1)=1$, it follows that both $\exp(-2\pi ic\gamma_1/m_1)$ and $\exp(2\pi ic\gamma_1/m_1)$ run over all primitive m_1-th roots of unity. Hence the right member of (1.23) becomes

$$\prod_{\substack{0<b<D/2\\(b,D)=1}} \prod'_{\rho(m_1)} (1-\rho x'^{mD+b})^{-1}(1-\rho x'^{mD+D-b})^{-1} = \prod_{\substack{0<b<D\\(b,D)=1}} \prod'_{\rho(m_1)} (1-\rho x'^{mD+b})^{-1},$$

where $\prod'_{\rho(m_1)}$ denotes that ρ ranges over all primitive m_1-th roots of unity.[5] Therefore, by (1.22),

$$\begin{aligned}\prod_{a\in\mathfrak{A}} F(x';b,D,\rho_a) &= \prod_{m=0}^{\infty} \prod_{\substack{0<b<D\\(b,D)=1}} \prod'_{\rho(m_1)} (1-\rho x'^{mD+b})^{-1} \\ &= \prod_{\substack{l=1\\(l,D)=1}}^{\infty} \prod'_{\rho(m_1)} (1-\rho x'^{l})^{-1}.\end{aligned} \tag{1.24}$$

We now use Lemma 1.2), substituting $f(t)=(1-e^{2\pi it}x'^{l})^{-1}$, $N=m_1$; thus

$$\prod'_{\rho(m_1)} (1-\rho x'^{l})^{-1} = \prod_{d|m_1} \{\prod_{\rho(d)} (1-\rho x'^{l})^{-1}\}^{\mu(m_1/d)},$$

where $\prod_{\rho(d)}$ denotes that ρ ranges over all d-th roots of unity. Since $\prod_{\rho(d)} (1-\rho x'^{l})^{-1} = (1-x'^{ld})^{-1}$, we have

$$\prod'_{\rho(m_1)} (1-\rho x'^{l})^{-1} = \prod_{d|m_1} (1-x'^{ld})^{-\mu(m_1/d)}.$$

The right member of (1.24) is therefore

$$\prod_{\substack{l=1\\(l,D)=1}}^{\infty} \prod_{d|m_1} (1-x'^{ld})^{-\mu(m_1/d)}.$$

Using Lemma 1.3), this becomes

$$\prod_{n=1}^{\infty} \prod_{d'|D} \prod_{d|m_1} (1-x'^{nd'd})^{-\mu(m_1/d)\mu(d')}. \tag{1.25}$$

Here we have

$$\mu(m_1/d)\mu(d') = \mu(m_1)\mu(d)\mu(d') = \epsilon\mu(dd') \qquad (\epsilon = \mu(m_1)).$$

Now, since $(D,m_1)=1$, we see that as d' runs over all divisors of D, and d over all divisors of m_1, $d'd$ runs just over all distinct divisors of Dm_1 $(=M)$. Accordingly, writing d instead of $d'd$, (1.25) reduces to

$$\prod_{n=1}^{\infty} \prod_{d|M} (1-x'^{nd})^{-\epsilon\mu(d)},$$

which furthermore is written, by using again Lemma 1.3), in the form

$$\prod_{\substack{l=1\\(l,M)=1}}^{\infty} (1-x'^{l})^{-\epsilon}. \tag{1.26}$$

---

[5] This notation will be also used in Cases ii) and iii) below.

The right member of (1.24) now turns out to be equal to (1.26), which in turn is identical with $F_{M^\epsilon}(x')$; consequently

$$(1.27)\qquad \prod_{a\in\mathfrak{A}} F(x';b,D,\rho_a)=F_{M^\epsilon}(x').$$

Inserting (1.18), (1.19), (1.21), (1.27) into (1.15), we are led to the transformation formula (1.2) for $D\geqq 3$.

Case ii). $D=2$. In this case we have always $b=1$, and so

$$\begin{aligned}\prod_{a\in\mathfrak{A}} F(x';b,D,\rho_a)&=\prod_{a\in\mathfrak{A}} F(x';1,2,\rho_a)\\ (1.28)\qquad &=\prod_{m=0}^{\infty}\prod_{a\in\mathfrak{A}}(1-\rho_a x'^{2m+1})^{-1}(1-\rho_a^{-1}x'^{2m+1})^{-1},\end{aligned}$$

Here $\rho_a=\exp(-2\pi ia\gamma/M)$, and γ, δ are given by $\gamma k_1-\delta m_1=1$. Now, let $\gamma\equiv 0 \pmod 2$ and put $\gamma=2\gamma_1$, so that $\gamma_1 k-\delta m_1=1$. H is then determined by $m_1 hH\equiv -1 \pmod k$, a congruence given in (1.1). Since $M=2m_1$, we have $\rho_a=\exp(-2\pi ia\gamma_1/m_1)$, where $(\gamma_1,m_1)=1$.

Now the integers $a_1,a_2,\cdots,a_K$, which constitute the set $\mathfrak{A}$, are pairwise incomplementary with respect to m_1. For if we assume, for instance, that $a_1+a_2=m_1$, then m_1 must be an even integer; indeed a_1 and a_2 are both odd since M is even. But the relation $M=2m_1$ shows that m_1 should be odd, contradicting the above. In addition, we have $0<a<m_1$ $(=M/2)$ $(a\in\mathfrak{A})$ by definition. Hence the integers a, m_1-a $(a\in\mathfrak{A})$ are distinct, the number of which being $\phi(M)=\phi(m_1)$, and belong to the interval $(0,m_1)$. This shows that these integers form a reduced residue system modulo m_1. Therefore the aggregate of the numbers ρ_a, ρ_a^{-1} $(a\in\mathfrak{A})$ coincides with the set of all primitive m_1-th roots of unity. Thus we obtain

$$\begin{aligned}&\prod_{m=0}^{\infty}\prod_{a\in\mathfrak{A}}(1-\rho_a x'^{2m+1})^{-1}(1-\rho_a^{-1}x'^{2m+1})^{-1}\\ &\qquad=\prod_{m=0}^{\infty}\prod_{\rho(m_1)}{}'(1-\rho x'^{2m+1})^{-1}=\prod_{\substack{l=1\\(l,2)=1}}^{\infty}\prod_{\rho(m_1)}{}'(1-\rho x'^{l})^{-1}.\end{aligned}$$

The last expression simplifies to $F_{M^\epsilon}(x')$ $(\epsilon=\mu(m_1))$ as in Case i). Consequently, by (1.28),

$$(1.29)\qquad \prod_{a\in\mathfrak{A}} F(x';b,D,\rho_a)=F_{M^\epsilon}(x').$$

From (1.15), (1.18), (1.19), (1.21), (1.29), it follows that the formula (1.2) is valid for $D=2$.

Case iii). $D=1$. In (1.16), the number ξ_a is defined by (1.14), and $\rho_a=\exp(-2\pi i\xi_a/M)$. Here ξ_a runs, as a does, over a set of $\phi(M)/2$ integers which are distinct, prime to M, and pairwise incomplementary with respect to M. Hence we get

$$(1.30) \qquad \prod_{a\in\mathfrak{A}} \tfrac{1}{2}\csc(\pi\xi_a/M) = \{ \prod_{\substack{0<r<M\\(r,M)=1}} \tfrac{1}{2}\csc(\pi r/M)\}^{\frac{1}{2}}$$

and

$$(1.31) \qquad \prod_{a\in\mathfrak{A}} (1-\rho_a x'^m)^{-1}(1-\rho_a^{-1}x'^m)^{-1} = \prod_{\rho(M)}{}' (1-\rho x'^m)^{-1}.$$

To evaluate the right member of (1.30), we employ Lemma 1.2) with $N=M$, $f(t)=\frac{1}{2}\csc(\pi t)$ $(0<t<1)$, $f(1)=1$; we obtain

$$\begin{aligned}\prod_{\substack{0<r<M\\(r,M)=1}} \tfrac{1}{2}\csc(\pi r/M) &= \prod_{d|M} \{ \prod_{1\leqq r<d} \tfrac{1}{2}\csc(\pi r/d)\}^{\mu(M/d)}\\ &= \prod_{d|M} d^{-\mu(M/d)} = \prod_{d|M} (M/d)^{-\mu(d)} = \prod_{d|M} d^{\mu(d)}\\ &= \begin{cases} M^{-1}, & \text{if } M \text{ is a prime,}\\ 1, & \text{otherwise.}\end{cases}\end{aligned}$$

Thus, by (1.30),

$$(1.32) \qquad \prod_{a\in\mathfrak{A}} \tfrac{1}{2}\csc(\pi\xi_a/M) = \tau(M)$$

where

$$(1.33) \qquad \tau(M) = \begin{cases} M^{-\frac{1}{2}}, & \text{if } M \text{ is a prime,}\\ 1, & \text{otherwise.}\end{cases}$$

Also we have, as in Case i),

$$(1.34) \qquad \prod_{m=1}^{\infty} \prod_{\rho(M)}{}' (1-\rho x'^m)^{-1} = \prod_{\substack{l=1\\(l,M)=1}}^{\infty} (1-x'^l)^{-\epsilon} = F_M{}^{\epsilon}(x') \qquad (\epsilon=\mu(M)).$$

By (1.31), (1.34), we find that

$$(1.35) \qquad \prod_{a\in\mathfrak{A}} \prod_{m=1}^{\infty} (1-\rho_a x'^m)^{-1}(1-\rho_a^{-1}x'^m)^{-1} = F_M{}^{\epsilon}(x').$$

On combining (1.16), (1.18), (1.19), (1.21), (1.32), and (1.35), the desired formula (1.2) is proved for $D=1$.

We now turn to the proof of the case $M=2$ which we have excluded from the above arguments. Now Theorem 3 of [6] states that

$$F_2(x) = \tau(2,D)\,\omega^*(h,k)\exp\{(\pi/12k)\,(\mu(D)/m_1 z + z)\}F_2{}^{\epsilon}(x'),$$

where

$$x = \exp(2\pi i h/k - 2\pi z/k), \qquad x' = \exp(2\pi i H/k - 2\pi/Kz),$$
$$m_1 hH \equiv -1 \pmod{k}, \qquad \epsilon = \mu(m_1),$$

and

$$(1.36) \qquad \omega^*(h,k) = \exp\{2\pi i\sigma_1(h,k)\}$$

with

$$\sigma_1(h,k)=\begin{cases}\sum\limits_{\mu}((\mu/k))((h\mu/k)) & (\mu=1,5,9,\cdots,\ k-3),\ \text{if } 4\mid k,\\ \sum\limits_{\mu}((\mu/2k))((h\mu/k)) & (\mu=1,5,9,\cdots,2k-3),\ \text{if } 2\mid k \text{ and } 4\nmid k,\\ \sum\limits_{\mu}((\mu/4k))((h\mu/k)) & (\mu=1,5,9,\cdots,4k-3),\ \text{if } 2\nmid k.\end{cases}$$

Hence we have, as in (1.21),

$$\omega^*(h,k)=\exp\{\pi i\Sigma_2(h,k)\}=\Omega_2(h,k) \tag{1.37}$$

with the $\Sigma_2(h,k)$ defined in (1.6). The formula (1.2) therefore remains true for $M=2$.

The proof of Theorem 1 is thus complete in all cases.

2. Estimation of some exponential sum. Let us consider the following exponential sum:

$$S_k=S_k(n,\nu;s_1,s_2)=\sum_h{}'\,\Omega_M(h,k)\exp\{2\pi i(-nh+\nu H)/k\} \tag{2.1}$$
$$(h \bmod k,\ s_1\leqq(\bar{h})<s_2).$$

Here n, ν, s_1, s_2 are all integers with $n\geqq 0$, $\nu\geqq 0$, $0<s_2-s_1\leqq k$; H and $\Omega_M(h,k)$ are defined respectively by (1.1) and (1.4); $\bar{h}$ is any fixed solution of $h\bar{h}\equiv 1 \pmod{k}$; the notation $s_1\leqq(\bar{h})<s_2$ implies that there exists an integer t such that $t\equiv\bar{h} \pmod{k}$, $s_1\leqq t<s_2$; and the summation symbol $\sum\limits_h{}'$ denotes here and subsequently that h runs over any reduced residue system of the given modulus with various summation conditions indicated in parentheses. We see that each summand in S_k has a period k with respect to h, and hence the residue system modulo k over which the summation extends can be arbitrary.

We shall now establish the following theorem.

THEOREM 2. *The sum S_k defined by* (2.1) *is subject to the estimate*

$$|S_k|<Ck^{1-\alpha}(n+1)^{\beta}$$

for n nonnegative integers and $n\neq n_0$ if $n_0=\mu(M)\phi(M)/24$ is a positive integer. Here α, β are any numbers satisfying $0<\alpha<\beta<\frac{1}{2}$, and C a positive constant depending only on α, β and M.

Proof. Throughout the proof, we shall make free use of the results of [5; § 2, pp. 943-950], and the meaning of the unexplained notations in the proof will be the same as in [5].

It is convenient to divide the discussion into two cases according as $D > 1$ or $D = 1$.

Case (1). $D > 1$. In the first place, we notice that S_k is written in the form

$$S_k = \sum_{\substack{0<c<D \\ (c,D)=1}} \sum_h{}' \Omega_M(h,k) \exp\{2\pi i(-nh+\nu H)/k\} \tag{2.2}$$

$$(h \bmod k, h \equiv c \pmod{D}, s_1 \leqq (\bar{h}) < s_2).$$

Next, by (1.21), (1.20), (1.37), and (1.36), we have

$$\Omega_M(h,k) = \exp\{2\pi i\sigma^*(h,k)\}, \qquad \sigma^*(h,k) = \sum_{a\in\mathfrak{A}} \sigma_a(h,k), \tag{2.3}$$

where

$$\mathfrak{A} = \{a_1, a_2, \cdots, a_K\} \ (M \geqq 3), \qquad \mathfrak{A} = \{1\} \ (M = 2).$$

On the other hand, [5, p. 947] implies that[6]

$$\sigma_a(h,k) \equiv (U_a h + V_a H)/(gDk) + W_a \pmod{1}; \tag{2.4}$$

in which[7]

$$U_a = gD^2\gamma_1(aX + MY) - \Phi\delta\{2K^2 + 3K(2a - M) + A\},$$

$$V_a = -\Phi(B - k^2),$$

$$W_a = -(\gamma_1 k_1/4)(k + 2b - 2D) + \{(a\gamma_1/2M) + (3\Phi\delta m_1/gD)\}(2b - D)$$
$$\qquad - (g\Psi\delta/4)\{2a + 2M + (2b-1)m_1\},$$

γ_1, δ being integers so chosen that $\gamma_1 k - \delta m_1 = 1$.

Therefore we find that

$$\sigma^*(h,k) = \sum_{a\in\mathfrak{A}} \sigma_a(h,k) \equiv (U^*h + V^*H)/(gDk) + W^* \pmod{1}, \tag{2.5}$$

where $U^* = \sum_{a\in\mathfrak{A}} U_a$, $V^* = \sum_{a\in\mathfrak{A}} V_a$, $W^* = \sum_{a\in\mathfrak{A}} W_a$.

We note that when $h \equiv c \pmod{D}$, we have, by (1.10), $b \equiv ah \equiv ac \pmod{D}$, and hence $b = ac - D[ac/D]$.

Putting $\sum_{a\in\mathfrak{A}} a = a^*$, $\sum_{a\in\mathfrak{A}} b = b^* = b^*(c)$, $\sum_{a\in\mathfrak{A}} A = A^*$, $\sum_{a\in\mathfrak{A}} B = B^*$, we obtain the following result:

---

[6] In the special case $M = 2$, we must put instead $a = 1$, $M = 4$ in the subsequent formulae.

[7] Φ, Ψ are any fixed integers satisfying $f\Phi + gDk\Psi = 1$ (see [5; (2.22), p. 946]). These integers were denoted by ϕ, ψ in [5], but we have to use here different notation since ϕ stands for the Euler function.

$$(2.6) \qquad U^* = gD^2\gamma_1(a^*X + MY\phi(M)/2) - \Phi\delta\{\phi(M)K^2 + 3K(2a^* - M\phi(M)/2) + A^*\},$$

$$V^* = -\Phi(B^* - k^2\phi(M)/2),$$

$$(2.6) \qquad W^* = -(\gamma_1 k_1/4)(k\phi(M)/2 + 2b^* - D\phi(M)) + (\sum_{a\in\mathfrak{A}} ab)\gamma_1/M - a^*\gamma_1/(2m_1) + (3\Phi\delta m_1/gD)(2b^* - D\phi(M)/2) - (g\Psi\delta/4)\{2a^* + M\phi(M) + (2b^* - \phi(M)/2)m_1\} = W^*(c).$$

By (2.2), (2.3), (2.5) (see [5; (2.34), p. 948])

$$S_k = \sum_{\substack{0<c<D \\ (c,D)=1}} (gD)^{-1}\exp(2\pi i W^*(c)) \cdot \sum_{l=0}^{k-1} c_l \sum_h{}' \exp(2\pi i\{(U^* - gDn)h + (V^*\delta + gD(\nu\delta + l))\bar{h}\}/gDk)$$
$$(h \bmod gDk,\ h \equiv c \pmod{D}).$$

Denoting the innermost sum by $T_k(l, c)$, we may write

$$S_k = \sum_{\substack{0<c<D \\ (c,D)=1}} (gD)^{-1}\exp(2\pi i W^*(c)) \sum_{l=0}^{k-1} c_l T_k(l, c).$$

The sum $T_k(l, c)$ here is a generalized Kloosterman sum, and is known to admit of the estimate (see [1], [10], [11]):

$$|T_k(l, c)| < C_0(gDk)^{1-\alpha}(gDk, U^* - gDn)^{\beta},$$

where α, β are any numbers satisfying $0 < \alpha < \beta < \frac{1}{2}$, and C_0 is a positive constant depending only on α and β.

Accordingly

$$|S_k| \leqq \sum_{\substack{0<c<D \\ (c,D)=1}} (gD)^{-1} \sum_{l=0}^{k-1} |c_l|\,|T_k(l, c)|$$

$$(2.7) \qquad < \phi(D)(gD)^{-1}C_0(gDk)^{1-\alpha}(gDk, U^* - gDn)^{\beta} \sum_{l=0}^{k-1} |c_l|$$

$$< C_0\phi(D)(gD)^{-\alpha}k^{1-\alpha}(gDk, U^* - gDn)^{\beta}\log(4k).$$

Now, in (2.6) we have

$$gDX \equiv 0 \pmod{k}, \qquad gDY \equiv 0 \pmod{k} \qquad \text{(see [5, p. 949])},$$

and hence $U^* \equiv -\Phi\delta A^* \pmod{k}$. Then we get

$$(gDk, U^* - gDn) \leqq gD(k, U^* - gDn) = gD(k, -\Phi\delta A^* - gDn)$$
$$= gD(k, f\Phi\delta A^* + fgDn) = gD(k, \delta A^* + 12Dn)$$
$$(2.8) \qquad = gD(k, m_1\delta A^* + 12m_1Dn)$$
$$= gD(k, (\gamma_1 k - 1)A^* + 12Mn)$$
$$= gD(k, 12Mn - A^*) \leqq gD\,|12Mn - A^*|,$$

where the last inequality follows only when $12Mn - A^* \neq 0$. But, by (1.18) we have

$$12Mn - A^* = 12Mn - \tfrac{1}{2}M\mu(M)\phi(M) = \tfrac{1}{2}M(24n - \mu(M)\phi(M))$$

for $M \neq 4$, and

$$12Mn - A^* = 48n + 2$$

for $M = 4$. Hence $12Mn - A^* \neq 0$ for $n \geqq 0$ and $n \neq n_0$ in case $n_0 = \mu(M)\phi(M)/24$ is a positive integer.

From (2.7) and (2.8), we derive further that

$$\begin{aligned} |S_k| &< C_0\phi(D)(gD)^{-\alpha}k^{1-\alpha}\{gD\,|12Mn - A^*|\}^{\beta}\log(4k) \\ &= O(k^{1-\alpha}(n+1)^{\beta}\log(4k)).^8 \end{aligned}$$

Here we can omit $\log(4k)$ from the O-term since we may choose α arbitrarily large so far as $\alpha < \beta$. This proves Theorem 2 for $D > 1$.

Case (2). $D = 1$. In the sum (2.1), the root of unity $\Omega_M(h,k)$ is also expressed by (2.3). Now let

$$\sigma_a'(h,k) = \sum_{\mu_a} (\mu_a/Mk - \tfrac{1}{2})(h\mu_a/k - [h\mu_a/k] - \tfrac{1}{2})$$
$$(\mu_a = a, M + a, 2M + a, \cdots, (k-1)M + a),$$

then we have

$$\sigma_a'(h,k) = \sigma_a(h,k) + (\tfrac{1}{2} - \xi_a/M)/2,$$

where ξ_a is defined in (1.14) (see [5; (3.17), p. 953]).

Consequently we obtain, in analogy with (2.4), the following result:

$$\sigma_a(h,k) \equiv (U_a h + V_a H)/(gk) + W_a' \pmod 1,$$

where

$$\begin{aligned} U_a &= g\gamma_1(aX + MY) - \Phi\delta\{2K^2 + 3K(2a - M) + A\}, \\ V_a &= -\Phi(1 - k^2), \\ W_a' &= -(\gamma_1 k/4)(k-2) - (a\gamma_1/2M) - (3\Phi\delta M/g) \\ &\qquad - (g\Psi\delta/4)(2a + M) + (\xi_a/M - \tfrac{1}{2})/2. \end{aligned}$$

We can therefore prove Theorem 2 in the case $D = 1$ by the same method as in Case (1).

3. Convergent series for the partition function. In this section, we shall deal with the partition function $p_M(n)$ for $M \geqq 2$, $n \geqq 0$, and $n \neq n_0$ if $n_0 = \mu(M)\phi(M)/24$ is a positive integer.

---

[8] We mean throughout the paper that the constant implied in the O-symbol always depends at most on α, β, and M.

We begin by representing $p_M(n)$ as a contour-integral:

$$p_M(n) = \frac{1}{2\pi i} \int_C x^{-n-1} F_M(x)\, dx,$$

where C is any circle with centre at $x = 0$ and radius less than unity. Taking C to be the circle $|x| = \exp(-2\pi N^{-2})$, where N is a natural number, and using the Farey dissection of order N, we obtain (see [9])

$$(3.1) \quad p_M(n) = \sum_{h,k}{}' \exp(-2\pi i n h/k) \int_{-\theta'}^{\theta''} F_M(\exp(2\pi i h/k - 2\pi w)) \exp(2\pi n w)\, d\theta$$
$$(0 \leqq h < k \leqq N;\ \theta' = \theta'_{h,k},\ \theta'' = \theta''_{h,k};\ w = N^{-2} - i\theta).$$

We now utilize the transformation formula (Theorem 1). By definition

$$F_M(x') = \sum_{\nu=0}^{\infty} p_M(\nu) x'^{\nu},$$

and furthermore we define the coefficients $q_M(\nu)$ in the power series expansion

$$F_M^{-1}(x') = \prod_{\substack{l=1 \\ (l,M)=1}}^{\infty} (1 - x'^{l}) = \sum_{\nu=0}^{\infty} q_M(\nu) x'^{\nu}.$$

It is evident that the $q_M(\nu)$ are all integers.

In the transformation formula (1.2), we substitute $z = kw$, and employ the above expansions. This gives us

$$\begin{aligned} &F_M(\exp(2\pi i h/k - 2\pi w)) \\ (3.2) \qquad &= \tau(M,D)\Omega_M(h,k)\exp\{(\pi\phi(M)/12k)(\mu(D)/Kw - \mu(M)kw)\} \\ &\qquad \cdot \sum_{\nu=0}^{\infty} \genfrac{}{}{0pt}{}{p_M}{q_M}(\nu) \exp(2\pi i \nu H/k - 2\pi\nu/Kkw), \end{aligned}$$

where

$$\genfrac{}{}{0pt}{}{p_M}{q_M}(\nu) = \begin{cases} p_M(\nu), & \text{if } \mu(m_1) = +1, \\ q_M(\nu), & \text{if } \mu(m_1) = -1. \end{cases}$$

Inserting (3.2) into (3.1) yields

$$\begin{aligned} p_M(n) &= \sum_{h,k}{}' \tau(M,D)\Omega_M(h,k)\exp(-2\pi i n h/k) \int_{-\theta'}^{\theta''} \sum_{\nu=0}^{\infty} \genfrac{}{}{0pt}{}{p_M}{q_M}(\nu) \\ (3.3) \qquad &\cdot \exp\{(\pi/12kKw)(\mu(D)\phi(M) - 24\nu) - (\pi w/12)(\mu(M)\phi(M) - 24n)\} \\ &\qquad \cdot \exp(2\pi i \nu H/k)\, d\theta. \end{aligned}$$

We separate here the sum over ν into two parts as

$$\sum_{\nu=0}^{\infty} = \sum_{\nu=0}^{\{\phi(M)/24\}} + \sum_{\nu > \{\phi(M)/24\}}$$

($\{t\}$ denotes the greatest integer less than t) so that the coefficient of w^{-1} is positive in the first sum when $\mu(D)=+1$, while it is negative or zero in the second sum. The right member of (3.3) then splits into two parts according to the above separation. Let that one which corresponds to the first sum be $Q(n)$, and let the other be $R(n)$. Then it will be established without difficulty, though we omit here the details, that, by using the method of Rademacher [9] and applying the estimation in Theorem 2, one can obtain the following result:

$$p_M(n)=Q(n)+R(n), \tag{3.4}$$

$$Q(n)=2\pi\sum_{\substack{k=1\\ \mu(D)=1}}^{N}\tau(M,D)\sum_{\nu=0}^{\{\phi(M)/24\}}\frac{p_M}{q_M}(\nu)S_k(n,\nu)L_k(n,\nu) + O(N^{-\alpha}(n+1)^{\beta}\exp(2\pi nN^{-2})), \tag{3.5}$$

$$R(n)=O(N^{-\alpha}(n+1)^{\beta}\exp(2\pi nN^{-2})), \tag{3.6}$$

where

$$S_k(n,\nu)=S_k(n,\nu;0,k)=\sum_{h \bmod k}{}' \Omega_M(h,k)\exp\{2\pi i(-nh+\nu H)/k\} \tag{3.7}$$

(see (2.1)) and

$$\begin{aligned} &L_k(n,\nu)\\ &=\frac{1}{2\pi i}\int^{(0+)}\exp\{(\pi/12kKw)(\phi(M)-24\nu)-(\pi w/12)(\mu(M)\phi(M)-24n)\}dw\\ &=\begin{cases} (kK)^{-\frac12}(\phi(M)-24n)^{-\frac12}(\phi(M)-24\nu)^{\frac12}\\ \qquad\cdot J_1((\pi/6(kK)^{\frac12})(\phi(M)-24n)^{\frac12}(\phi(M)-24\nu)^{\frac12})\\ \qquad\qquad\text{if } \mu(M)=1 \text{ and } n<\phi(M)/24,\\ (kK)^{-\frac12}(24n-\mu(M)\phi(M))^{-\frac12}(\phi(M)-24\nu)^{\frac12}\\ \qquad\cdot I_1((\pi/6(kK)^{\frac12})(24n-\mu(M)\phi(M))^{\frac12}(\phi(M)-24\nu)^{\frac12})\\ \qquad\qquad\text{if } n>\mu(M)\phi(M)/24, \end{cases} \end{aligned} \tag{3.8}$$

$J_1(t)$, $I_1(t)$ being Bessel functions of the first order.

Now, when $\mu(D)=1$ we have $\tau(M,D)=\tau(M)$ (see (1.3), (1.33)) and $\mu(m_1)=\mu(M)$, and so we may write (3.5) in the form

$$Q(n)=2\pi\tau(M)\sum_{\substack{k=1\\ \mu(D)=1}}^{N}\sum_{\nu=0}^{\{\phi(M)/24\}}r_M(\nu)S_k(n,\nu)L_k(n,\nu) + O(N^{-\alpha}(n+1)^{\beta}\exp(2\pi nN^{-2})) \tag{3.9}$$

with the notation

$$r_M(\nu)=\begin{cases} p_M(\nu), & \text{if } \mu(M)=+1,\\ q_M(\nu), & \text{if } \mu(M)=-1. \end{cases} \tag{3.10}$$

In (3.4), (3.9), and (3.6), we keep n fixed and let $N \to \infty$; we thus obtain:

THEOREM 3. *If $p_M(n)$ denotes the number of partitions of n into positive summands prime to M, where M is a square-free number $\geqq 2$, then we have, for $n \geqq 0$ and $n \neq n_0$ (in case $n_0 = \mu(M)\phi(M)/24$ is a positive integer), the convergent series representation*[9]

$$p_M(n) = 2\pi\tau(M) \sum_{\substack{k=1 \\ \mu(D)=1}}^{\infty} \sum_{\nu=0}^{\{\phi(M)/24\}} r_M(\nu) S_k(n,\nu) L_k(n,\nu). \tag{3.11}$$

References to the meaning of the symbols $\tau(M)$, $r_M(\nu)$, $S_k(n,\nu)$, and $L_k(n,\nu)$ are given in (1.33), (3.10), (3.7), *and* (3.8) *respectively.*

4. Asymptotic formulae for the partition function.

We quote here two lemmas from [5, p. 956].

LEMMA 4.1. *Let $I_1(t)$ be the Bessel function of the first order with purely imaginary argument. Then*

(4.1) $\quad I_1(t)$ *is positive and increasing for* $t > 0$,

$$I_1(t) = O(t) \quad (t \to 0), \tag{4.2}$$

$$I_1(t) = (2\pi t)^{-\frac{1}{2}} e^t (1 + O(t^{-1})) \quad (t \to +\infty). \tag{4.3}$$

LEMMA 4.2. *Let R be a real number $\geqq 2$, and define*

$$S_1(R) = \sum_{\nu=1}^{\leqq R} \nu^{\frac{1}{2}} e^{R/\nu}, \qquad S_2(R) = \sum_{\nu=2}^{\leqq R} \nu^{\frac{1}{2}} e^{R/\nu}.$$

Then $S_1(R) < 2e^R$ for $R \geqq 6$, and $S_2(R) < 5e^{\frac{1}{2}R}$ for $R \geqq 12$.

We shall now investigate the asymptotic behavior of $p_M(n)$ as n becomes large and M is fixed.

It is easy to see that in (3.11) of Theorem 3, the summation over k can be written in the form

$$\sum_{\substack{k=1 \\ \mu(D)=1}}^{\infty} = \sum_{\substack{D|M \\ \mu(D)=1}} \sum_{\substack{k_1=1 \\ (k_1,m_1)=1}}^{\infty} = \sum_{\substack{k=1 \\ (k,M)=1}}^{\infty} + \sum_{\substack{D|M,D\geqq 6 \\ \mu(D)=1}} \sum_{\substack{k_1=1 \\ (k_1,m_1)=1}}^{\infty} \tag{4.4}$$

where $k = k_1 D$, $M = m_1 D$, and we have used the fact that $D > 1$ and $\mu(D) = 1$ together imply that $D \geqq 6$. The right member of (3.11) then divides into two parts according to the separation on the extreme right of (4.4). These parts will be denoted by $p_M^{(1)}(n)$ and $p_M^{(2)}(n)$, namely,

---

[9] The series for $p_M(n)$ is in fact *absolutely* convergent, as may be seen from arguments in the next section.

$$(4.5) \qquad p_M(n) = p_M^{(1)}(n) + p_M^{(2)}(n),$$

$$(4.6) \qquad p_M^{(1)}(n) = 2\pi\tau(M) \sum_{\substack{k=1 \\ (k,M)=1}}^{\infty} \sum_{\nu=0}^{\{\phi(M)/24\}} r_M(\nu) S_k(n,\nu) L_k(n,\nu),$$

$$(4.7) \qquad p_M^{(2)}(n) = 2\pi\tau(M) \sum_{\substack{D|M, D\geqq 6 \\ \mu(D)=1}} \sum_{\substack{k_1=1 \\ (k_1,m_1)=1}}^{\infty} \sum_{\nu=0}^{\{\phi(M)/24\}} r_M(\nu) S_k(n,\nu) L_k(n,\nu).$$

Now, by (3.7) we have, since $\Omega_M(h,k)$ are roots of unity, the trivial estimate

$$(4.8) \qquad |S_k(n,\nu)| \leqq \sum_{h \bmod k}' 1 \leqq k.$$

On the other hand, by Theorem 2, we have the non-trivial estimate[10]

$$(4.9) \qquad |S_k(n,\nu)| < C_1 k^{1-\alpha}(n+1)^{\beta} \quad (0 < \alpha < \beta < \tfrac{1}{2}).$$

Next, by (3.8) we may write

$$(4.10) \quad L_k(n,\nu) = (kK)^{-\frac{1}{2}} E^{-1} (\phi(M) - 24\nu)^{\frac{1}{2}} I_1((\pi E/6(kK)^{\frac{1}{2}})(\phi(M) - 24\nu)^{\frac{1}{2}})$$

with the abbreviation

$$(4.11) \qquad E = (24n - \mu(M)\phi(M))^{\frac{1}{2}} \qquad (n > \phi(M)/24).$$

Also we have

$$(4.12) \qquad kK = k_1^2 DM$$

since $k = k_1 D$, $K = k_1 M$.

From (4.1), (4.8), (4.9), (4.10), (4.12) we deduce

$$(4.13) \qquad \left| \sum_{\nu=0}^{\{\phi(M)/24\}} r_M(\nu) S_k(n,\nu) L_k(n,\nu) \right| \leqq \begin{cases} E^{-1} Z_M I_1(F/k_1), \\ C_1 E^{-1} Z_M (n+1)^{\beta} k_1^{-\alpha} I_1(F/k_1), \end{cases}$$

where

$$Z_M = \sum_{\nu=0}^{\{\phi(M)/24\}} |r_M(\nu)| (\phi(M) - 24\nu)^{\frac{1}{2}}$$

and

$$(4.14) \qquad F = (\pi E/6D^{\frac{1}{2}})(\phi(M)/M)^{\frac{1}{2}}.$$

Let us deal with $p_M^{(2)}(n)$ first. By (4.7), (4.13), (4.2), (4.3), and Lemma 4.2, we get

---

[10] In what follows we shall use $C_1, C_2, \cdots, C_{15}$ to denote certain positive constants depending at most on α, β, and M.

$$
\begin{aligned}
|p_M^{(2)}(n)| &< 2\pi\tau(M) \sum_{\substack{D|M, D\geqq 6\\ \mu(D)=1}} \sum_{k_1=1}^{\leqq F} C_2 E^{-1} F^{-\frac12} k_1^{\frac12} e^{F/k_1} \\
(4.15)\qquad &\quad + 2\pi\tau(M) \sum_{\substack{D|M, D\geqq 6\\ \mu(D)=1}} \sum_{k_1>F} C_3 E^{-1}(n+1)^{\beta} F k_1^{-1-\alpha} \\
&< C_4 E^{-1} \sum_{\substack{D|M, D\geqq 6\\ \mu(D)=1}} F^{-\frac12} e^{F} + C_5 E^{-1}(n+1)^{\beta} \sum_{\substack{D|M, D\geqq 6\\ \mu(D)=1}} F^{1-\alpha}.
\end{aligned}
$$

Now set

$$(4.16)\qquad G = (\pi E/6)(\phi(M)/M)^{\frac12} = (\pi/6)(\phi(M)/M)^{\frac12}(24n - \mu(M)\phi(M))^{\frac12}.$$

Then, by (4.14), we have $F = D^{-\frac12}G$. Moreover, since $6 \leqq D \leqq M$, we find that $M^{-\frac12}G \leqq F \leqq 6^{-\frac12}G$. Hence, by (4.15),

$$(4.17)\qquad |p_M^{(2)}(n)| < C_6 E^{-1} G^{-\frac12} \exp(6^{-\frac12}G) + C_7 E^{-1}(n+1)^{\beta} G^{1-\alpha}.$$

We next treat $p_M^{(1)}(n)$. On the right-hand side of (4.6), we distinguish the term $k=1$ from the others, and observe that $S_1(n,\nu)=1$. This yields

$$
\begin{aligned}
(4.18)\qquad p_M^{(1)}(n) &= 2\pi\tau(M) \sum_{\nu=0}^{\{\phi(M)/24\}} r_M(\nu) L_1(n,\nu) + u(n), \\
u(n) &= 2\pi\tau(M) \sum_{\substack{k>1\\ (k,M)=1}} \sum_{\nu=0}^{\{\phi(M)/24\}} r_M(\nu) S_k(n,\nu) L_k(n,\nu).
\end{aligned}
$$

Using (4.13), (4.2), (4.3), and Lemma 4.2 (note that we have here $F=G$), we infer

$$
\begin{aligned}
|u(n)| &< 2\pi\tau(M) \sum_{k=2}^{\leqq G} C_8 E^{-1} G^{-\frac12} k^{\frac12} e^{G/k} \\
(4.19)\qquad &\quad + 2\pi\tau(M) \sum_{k>G} C_9 E^{-1}(n+1)^{\beta} G k^{-1-\alpha} \\
&< C_{10} E^{-1} G^{-\frac12} e^{\frac12 G} + C_{11} E^{-1}(n+1)^{\beta} G^{1-\alpha}.
\end{aligned}
$$

Noting that $\frac12 > 6^{-\frac12}$, we have, from (4.17), (4.19),

$$(4.20)\qquad |p_M^{(2)}(n) + u(n)| < C_{12} E^{-1} G^{-\frac12} e^{\frac12 G} + C_{13} E^{-1}(n+1)^{\beta} G^{1-\alpha}.$$

Next, in the sum over ν on the right of (4.18), we separate the term $\nu=0$ from the others, and obtain

$$
\begin{aligned}
(4.21)\qquad & 2\pi\tau(M) \sum_{\nu=0}^{\{\phi(M)/24\}} r_M(\nu) L_1(n,\nu) \\
&= 2\pi\tau(M) L_1(n,0) + 2\pi\tau(M) \sum_{\nu=1}^{\{\phi(M)/24\}} r_M(\nu) L_1(n,\nu),
\end{aligned}
$$

where the second term on the right side occurs only when $\phi(M) > 24$.

Now we have

$$(4.22) \qquad L_1(n,\nu) = M^{-\frac{1}{2}}E^{-1}(\phi(M)-24\nu)^{\frac{1}{2}}I_1((\pi E/6M^{\frac{1}{2}})(\phi(M)-24\nu)^{\frac{1}{2}})$$

by (4.10). Also, by (4.16),

$$(\pi E/6M^{\frac{1}{2}})(\phi(M)-24)^{\frac{1}{2}} = G(1-24/\phi(M))^{\frac{1}{2}} = GM_1,$$

where

$$(4.23) \qquad M_1 = (1-24/\phi(M))^{\frac{1}{2}} < 1 \qquad (\phi(M) > 24).$$

Therefore, using (4.1), (4.3), we derive

$$(4.24) \qquad \begin{aligned} \Big|\sum_{\nu=1}^{\{\phi(M)/24\}} r_M(\nu)L_1(n,\nu)\Big| &< C_{14}E^{-1}I_1((\pi E/6M^{\frac{1}{2}})(\phi(M)-24)^{\frac{1}{2}}) \\ &< C_{15}E^{-1}G^{-\frac{1}{2}}e^{GM_1}. \end{aligned}$$

On the other hand, from (4.22), (4.16), and (4.3) we see that

$$(4.25) \qquad \begin{aligned} L_1(n,0) &= (\phi(M)/M)^{\frac{1}{2}}E^{-1}I_1(G) \\ &= (\phi(M)/M)^{\frac{1}{2}}E^{-1}(2\pi G)^{-\frac{1}{2}}e^{G}(1+O(G^{-1})). \end{aligned}$$

It now follows from (4.5), (4.18), (4.20), (4.21), (4.24), and (4.25) that

$$(4.26) \qquad \begin{aligned} p_M(n) &= 2\pi\tau(M)(\phi(M)/M)^{\frac{1}{2}}E^{-1}I_1(G) \\ &\quad \cdot\{1+O(e^{GM_1-G})+O(e^{-\frac{1}{2}G})+O((n+1)^{\beta}G^{\frac{3}{2}-\alpha}e^{-G})\}. \end{aligned}$$

But we have $\frac{1}{2} \underset{>}{\leqq} 1-M_1$ according as $\phi(M) \underset{>}{\leqq} 32$, and so, by (4.26) and (4.16),

$$(4.27) \qquad p_M(n) = 2\pi\tau(M)(\phi(M)/M)^{\frac{1}{2}}E^{-1}I_1(G)\{1+O(\exp(-cn^{\frac{1}{2}}))\},$$

where c is a positive constant defined by

$$(4.28) \qquad c = 2\pi(\phi(M)/6M)^{\frac{1}{2}}c', \qquad c' = \begin{cases} \frac{1}{2}, & \text{if } \phi(M) \leqq 32, \\ 1-M_1, & \text{if } \phi(M) > 32, \end{cases}$$

with the M_1 of (4.23).

Substitution of (4.11) and (4.16) into (4.27) yields the following

THEOREM 4. *We have, as* $n \to \infty$, *the asymptotic formula*

$$\begin{aligned} p_M(n) &= 2\pi\tau(M)(\phi(M)/M)^{\frac{1}{2}}(24n-\mu(M)\phi(M))^{-\frac{1}{2}} \\ &\quad \cdot I_1((\pi/6)(\phi(M)/M)^{\frac{1}{2}}(24n-\mu(M)\phi(M))^{\frac{1}{2}})\{1+O(\exp(-cn^{\frac{1}{2}}))\} \end{aligned}$$

with the constant c *of* (4.28).

From Theorem 4 and (4.3), we can easily find an asymptotic formula for $p_M(n)$ in terms of elementary functions of n; we have

$$p_M(n) = 2\cdot 3^{\frac{1}{2}}\tau(M)(\phi(M)/M)^{\frac{1}{4}}(24n-\mu(M)\phi(M))^{-\frac{3}{4}}$$
$$\cdot\exp((\pi/6)(\phi(M)/M)^{\frac{1}{2}}(24n-\mu(M)\phi(M))^{\frac{1}{2}})\{1+O(n^{-\frac{1}{2}})\},$$

which furthermore simplifies to

$$p_M(n) = \tfrac{1}{2}\tau(M)(\phi(M)/6M)^{\frac{1}{4}}n^{-\frac{3}{4}}\exp(2\pi(\phi(M)/6M)^{\frac{1}{2}}n^{\frac{1}{2}})\{1+O(n^{-\frac{1}{2}})\},$$

This formula will also be deduced, except for the order of its error term, from a result of Meinardus [7].

DEFENSE ACADEMY, YOKOSUKA, JAPAN.

REFERENCES.

[1] T. Estermann, "Vereinfachter Beweis eines Satzes von Kloosterman," *Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität*, vol. 7 (1929), pp. 82-98.

[2] E. Grosswald, "Some theorems concerning partitions," *Transactions of the American Mathematical Society*, vol. 89 (1958), pp. 113-128.

[3] M. Haberzetle, "On some partition functions," *American Journal of Mathematics*, vol. 63 (1941), pp. 589-599.

[4] L. K. Hua, "On the number of partitions of a number into unequal parts," *Transactions of the American Mathematical Society*, vol. 51 (1942), pp. 194-201.

[5] S. Iseki, "A partition function with some congruence condition," *American Journal of Mathematics*, vol. 81 (1959), pp. 939-961.

[6] ———, "Some transformation equations in the theory of partitions," *Proceedings of the Japan Academy*, vol. 34 (1958), pp. 131-135.

[7] G. Meinardus, "Asymptotische Aussagen über Partitionen," *Mathematische Zeitschrift*, vol. 59 (1954), pp. 388-398.

[8] I. Niven, "On a certain partition function," *American Journal of Mathematics*, vol. 62 (1940), pp. 353-364.

[9] H. Rademacher, "The Fourier coefficients of the modular invariant $J(\tau)$," *ibid.*, vol. 60 (1938), pp. 501-512.

[10] H. Salié, "Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen," *Mathematische Zeitschrift*, vol. 36 (1933), pp. 263-278.

[11] A. Weil, "On some exponential sums," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 34 (1948), pp. 204-207.

REGULARIZATION OF SINGULAR INTEGRAL OPERATORS ON COMPACT MANIFOLDS.*

By R. T. SEELEY.[1]

Introduction. An important technique in the use of singular integral operators is that known as regularization, which means roughly reduction to an ordinary integral. There seems to be no thorough investigation of this method for singular integral operators on manifolds, either for a single operator or for systems. This paper demonstrates that on compact manifolds of dimension two or more, for any elliptic singular integral operator H there is an invertible operator H' such that $H'H$ is the identity plus a completely continuous operator. Here "elliptic" means "with symbol never zero." The well-developed theory of singular integrals along plane curves shows that this result is not true for the circle, so that the restriction to dimension two or more is essential.

The last section of the paper develops theorems of Fredholm type for singular integral operators, along with some results on the smoothness of solutions of singular integral equations.

The author is grateful to a number of people for helpful discussions about the topological aspects of the problem, particularly A. P. Calderon, R. K. Lashof, and Richard Swan. This side of the problem is treated fully here, while the analytic side is presented only summarily, relying on [4] for details.

1. In this section we summarize, with slight changes, the relevant results for singular integral operators as developed in [4]; and we state the main results of the present paper. M will consistently denote a compact manifold of class $r \geqq 3$, of dimension $k \geqq 2$, and with a Riemannian metric of class $r-1$. C_m denotes the functions of class $m \leqq r$ on M, i.e. functions whose derivatives of order m, with respect to any local coordinates, are continuous. C_β denotes the functions of class $[\beta]$ whose derivatives of order $[\beta]$ satisfy a uniform Hölder condition with exponent $\beta-[\beta]$; here $[\beta]$ is the largest integer $\leqq \beta$.

---

* Received November 25, 1960.

[1] A large part of the work on this paper was done while the author was temporarily employed by the University of Chicago and by Massachusetts Institute of Technology.

In the definition of singular integral operators we use the space of functions with Schwartz distribution derivatives of order $\leqq n$ in L^p, for which we use the notation L_n^p. These can be defined and given a norm by the use of a resolution of the identity $\sum \phi^i = 1$, in which each ϕ^i is $\geqq 0$, in C_r, and has support in a simply connected coordinate neighborhood U_i with coordinates x^i (x^i denoting the k real-valued coordinate functions $x_1^i, \cdots, x_k^i$) mapping U_i onto the open set G_i in E_k, k-space. If f is a function on M, let f_i denote the function on G_i given by $f_i(y) = f(x^{-1}(y))$, where x^{-1} denotes the inverse of the mapping x^i. Then we say that f is in L_n^p $(n \leqq r)$ if and only if for each i, f_i is in $L_n^p(G_i)$. A norm can be introduced in L_n^p by

$$\| f \|_{n,p} = \Big(\sum_{|\alpha| \leqq n} \sum_i \| (\phi^i{}_i)^{1/p} (\partial/\partial y)^\alpha f_i \|^p \Big)^{1/p}$$

where $\| g \|$ denotes the L^p norm of g on E_k. Here $\alpha = (\alpha_1, \cdots, \alpha_k)$, the α_i are non-negative integers, $|\alpha| = \sum \alpha_i$, and $(\partial/\partial y)^\alpha = \partial^{|\alpha|}/\partial y_1^{\alpha_1} \cdots \partial y_k^{\alpha_k}$. An operator T on $L^p(M)$ $(1 < p < \infty)$ is *smoothing of order* n if, for each non-negative integer $m < n$, T is bounded from L_m^p to L_{m+1}^p, and T^* is bounded from L_m^q to L_{m+1}^q $(1/p + 1/q = 1)$. If ϕ is a function on M with support in a neighborhood U with coordinates x, then ϕ_x denotes the transformation which takes functions f on M into functions $\phi_x f$ on E_k in such a way that $\phi_x f(y) = \phi(x^{-1}(y)) f(x^{-1}(y))$ whenever y is in the range of x, and $\phi_x f(y) = 0$ otherwise. Similarly ϕ^x transforms functions g on E_k into functions $\phi^x g$ on M in such a way that $\phi^x g(m) = \phi(m) g(x(m))$ for any m in M.

Definition 1. An operator T on $L^p(M)$ is of type $C_\beta{}^\infty$ $(\beta \leqq n-1)$ if and only if it satisfies the following conditions.

i) For each ϕ and ψ in C_r with disjoint (compact) support, the operator $\phi T \psi$ given by $(\phi T \psi) f = \phi \cdot T(\psi \cdot f)$ is completely continuous and smoothing of order $[\beta]$ on all $L^p(M)$, $1 < p < \infty$. Here $f \cdot g$ indicates the pointwise multiplication of the functions f and g, and $[\beta]$ indicates the largest integer $\leqq \beta$.

ii) For each ϕ and ψ with (compact) support in the same coordinate neighborhood with coordinates x, $\phi T \psi = \phi^x H \psi_x + R$, where H is a singular integral operator on E_k of type $C_\beta{}^\infty$, in the sense of Calderon and Zygmund [1],

$$Hf(y) = a(y) f(y) + \lim_{\epsilon \to 0} \int_{|y-z| > \epsilon} h(y, y-z) f(z)\, dz;$$

and R is completely continuous and smoothing of order $[\beta]$ on all $L^p(M)$, $1 < p < \infty$.

The coordinates x give rise to a basis for the tangent plane at any point m in their domain; the members of this basis are indicated in a natural way by $\partial/\partial x_1, \cdots, \partial/\partial x_k$. The metric on M gives an inner product (ξ, η) on each tangent plane. The dual space to the tangent plane at m, which we call the co-tangent plane, has the dual basis denoted by $dx_1, \cdots, dx_k$, and a dual inner product denoted by (ξ', η'). With this notation, the function $h(x, z)$ on $E_k \times E_k$ appearing in Definition 1 gives rise to a function $\bar{h}$ on the part of the tangent bundle over the domain of the coordinates x, $\bar{h}(m, \Sigma z_i \partial/\partial x_i) = h(x(m), z)$. Its principal value Fourier transform with respect to z appears naturally as a function on part of the bundle of cotangent planes, whose value at $(m, \Sigma \xi_i dx_i)$ is given by

$$\lim_{\epsilon \to 0} \int_{\epsilon^{-1} > |z| > \epsilon} \exp(i \Sigma \xi_j z_j) h(x(m), z) \, dz.$$

This function is positively homogeneous of degree zero in the ξ_i, and all derivatives with respect to the ξ_i are in C_β on the part of the cotangent bundle where the function is defined and where $\Sigma \xi_i^2 \geqq 1$.

By the cosphere bundle $CS(M)$ we mean the bundle obtained by considering the subset of the cotangent bundle consisting of all cotangent vectors whose Riemannian length $(\Sigma \xi_i dx_i, \Sigma \xi_i dx_i)^{\frac{1}{2}}$ equals one. Then the function described immediately above is determined by its values on $CS(M)$. We call a function on $CS(M)$ of type C_β^∞ if and only if, after being extended over each cotangent plane so as to be positively homogeneous of degree zero, it has on each cotangent plane derivatives of all orders with respect to the variables ξ_i arising from a coordinate system x, and these derivatives are in C_β on the part of the cotangent bundle over the domain of x where $\Sigma \xi_i^2 \geqq 1$.

Definition 2. The symbol of a C_β^∞ operator T is the function on $CS(M)$ defined by $\sigma(T)(m, \Sigma \xi_i dx_i) = a(x(m)) + \lim_{\epsilon \to 0} \int_{\epsilon^{-1} > |z| > \epsilon} \exp(i \Sigma \xi_j z_j) h(x(m), z) \, dz$, where x, a, and h are the functions in Definition 1, $z = (z_1, \cdots, z_k)$, $|z|^2 = \Sigma z_i^2$, and $\phi(m) \psi(m) \neq 0$.

It is shown in [4] that the function thus defined depends only on T, and not on any of the intermediate functions x, a, or h. The above discussion asserts that it is of type C_β^∞. The symbol thus defined for C_β^∞ operators has the following properties.

i) $\sigma(T) \equiv 0$ if and only if T is completely continuous and smoothing of order $[\beta]$.

ii) If $\beta \neq 1$, the C_β^∞ operators form a self-adjoint algebra, and σ is a homomorphism of this algebra onto the algebra of functions on $CS(M)$ of type C_β^∞, such that $\sigma(T^*)$ is the complex conjugate of $\sigma(T)$.

iii) In [4], Theorem 2, the "onto" part of assertion (ii) is proved by constructing an operator with prescribed symbol. In what we do here it is important to have an estimate of the norm of this operator in terms of the symbol. The complete derivation of such an estimate, based on the corresponding result for operators on Euclidean space, is more tedious than enlightening. We shall only state carefully the form of an estimate based on the resolution $\Sigma\phi^i = 1$ and the coordinates x^i introduced above to define the norm on L_n^p. Suppose $F(m,\eta)$ is a function on the cotangent bundle, homogeneous of degree zero on each cotangent plane, whose restriction to $CS(M)$ is of type C_β^∞. Let N_i denote an upper bound for $\phi^i(m)F(m, \Sigma\xi_j dx_j^i)$ and its derivatives of order $2k$ with respect to the ξ_j, evaluated in $\Sigma\xi_j^2 \geqq 1$. Let $N = \max N_i$. Then there is a constant K depending only on the ϕ^i and x^i, and a constant A_p depending only on p and the dimension of M, such that if T is the operator constructed in Theorem 2 of [4] with $\sigma(T) = F$, then $\| T \|_p \leqq NKA_p$.

Because of the relation of the symbol of a C_β^∞ operator to the characteristic polynomial of a differential operator (see [1], Theorem 7, and [4], Theorem 6) we make the following

Definition 3. A function F on $CS(M)$ is called elliptic if and only if it never vanishes. A C_β^∞ operator is elliptic if and only if its symbol is elliptic.

The main result of the present paper is

THEOREM 1. *If $\beta \neq 1$ and $F(m,\eta)$ is an ellpitic C_β^∞ function on $CS(M)$, then for each p in $1 < p < \infty$ there is a C_β^∞ operator T with $\sigma(T) = F$, and such that T is invertible when operating on L^p.*

2. This section establishes the basic lemma for our approach, Lemma 3, and completes the proof of Theorem 1 for $\dim(M) > 2$. Here p and β are fixed numbers, $\beta \neq 1$, $\beta \geqq 0$, and $1 < p < \infty$; and $\| A \|$ denotes the norm of A operating on L^p. As a formal convenience we introduce the class P of symbols of C_β^∞ operators which are invertible on L^p, and show that if F is elliptic then F is in P. Clearly P is closed under multiplication; and if $F(m,\eta)$ is elliptic, in C_β^∞, and independent of η, then F is the symbol of the operator consisting of multiplication by $F(m,\eta)$ and hence is in P.

LEMMA 1. *Let $F(m,\eta)$, N, K, and A_p, be as in the discussion of property*

(iii) *of Section* 1 *above. Then if* $|1-F| < (A_pK)^{-1}$ *and* $N < (A_pK)^{-1}$, F *is in* P.

The proof is obvious: under these conditions it is possible to choose a C_β^∞ operator T_1 with $\sigma(T_1) = 1 - F$ and $\| T_1 \| < 1$. Then let $T = I - T_1$, I the identity operator.

LEMMA 2. *If the complex argument of* F *can be defined continuously on each individual cosphere, and* F_1 *is the function on the cosphere bundle whose absolute value and argument on each cosphere are the averages respectively of the absolute value and argument of* F *on that cosphere, then* F *is homotopic to* F_1 *by a homotopy* F_t *such that* $\min |F_t| \geqq \min |F|$.

Proof. Construct on the cross product of the unit sphere in E_k with itself a kernel $K_t(Z, Z')$ with the folowing properties.

i) For each t, $K_t(Z,Z')$ depends only on the distance $d(Z,Z')$.

ii) $K_1(Z,Z')$ is constant.

iii) For $t > 0$, $K_t(Z,Z')$ is continuous in its three variables.

iv) For each $\epsilon > 0$, $\sup K_t(Z,Z')$ for $d(Z,Z') \geqq \epsilon$ tends to zero as $t \rightarrow 0$.

v) $K_t(Z,Z') \geqq 0$.

vi) $\int_{|Z'|=1} K_t(Z,Z')\,d\mu' = 1$. ($d\mu' =$ volume element on $|Z'| = 1$).

This, of course, can be done easily in a variety of ways. Now define F_t on the cosphere over the point m by $|F_t(m,\mu)| = \int K_t(\mu,\mu')|F(m,\mu')|\,d\mu'$, and $\arg F_t(m,\mu) = \int K_t(\mu,\mu') \arg F(m,\mu')\,d\mu'$, where $\arg F(m,\mu')$ is any continuous function on the cosphere over m for which $F = |F| \exp[i \arg F(m,\mu')]$. By property (i) of K_t, these integrals over the cosphere are independent of any choice of coordinates for the cosphere, and depend only on its metric and surface volume element as a unit sphere in E_k. Since the cosphere in question is connected ($\dim M \geqq 2$), any two continuous definitions of $\arg F$ differ by a constant $2\pi n$, so that by property (vi) of K_t, $\arg F_t$ is well defined mod 2π. Thus F_t is well defined. To see that it is continuous, define $\arg F$ continuously on the part of the cosphere bundle over a simply connected coordinate neighborhood on M; the F_t obtained from this as above has continuous argument and absolute value. It is clear from the properties assumed for K_t that $F_0 = F$, F_1 is as advertised, and $\min |F_t| \geqq \min |F|$.

LEMMA 3. *If* F *is elliptic and* $\arg F$ *can be defined continuously on each cosphere, then* F *is in* P.

Proof. Let F_1 be the function obtained from F in Lemma 2. Then F_1 is in P, since it is constant on each cosphere, and it is enough to show that F/F_1 is in P. But F/F_1 is homotopic to $F_1/F_1 \equiv 1$. Define $\arg(F_1/F_1) = 0$, and extend this argument function continuously to F_t/F_1 for $0 \leqq t \leqq 1$, (see next paragraph for details), obtaining a continuous $\arg(F/F_1)$ over the whole cosphere bundle. Then take n large enough that $(F/F_1)^{1/n}$ satisfies the hypotheses of Lemma 1, so that $(F/F_1)^{1/n}$ is in P. Since P is closed under multiplication, F/F_1 and F are in P.

To define $\arg(F_t/F_1)$ we rely on the "second covering homotopy theorem" in [5], page 54. In this case the reals form a bundle B' over the unit circle X', with $p(b) = e^{ib}$; and we are given a map $f_0 = \arg(F_1/F_1) = 0$ from the cosphere bundle X into B' along with a map $\bar{f} = F_t|F_1|/F_1|F_t|$ of $X \times I \rightarrow X'$ which is a homotopy of $p(f_0)$. The covering theorem asserts that there is a homotopy $f\colon X \times I \rightarrow B'$ which covers $\bar{f}$, i.e. a continuous definition of $\arg(F_t/F_1)$. Thus the lemma is proved.

Lemma 3 proves Theorem 1 in case $\dim(M) > 2$, since in this case the cospheres are simply connected and $\arg F$ can always be defined continuously over each one. Sections 3 and 4 below complete the discussion for $\dim(M) = 2$.

3. In this section we prove

LEMMA 4. *Suppose M is not a torus, $\dim(M) = 2$, and F is a continuous function from the tangent circle bundle of M to the complex unit circle. Then the restriction of F to any tangent circle has degree zero.*

This result shows that Lemma 3 applies directly to all manifolds except the torus, and hence completes the proof of Theorem 1 in those cases.

For non-orientable manifolds the proof of Lemma 4 is quite easy. Suppose F has non-zero degree on C^0, the tangent circle at $m_0 \in M$, and let m_1 be any other point in M. Connect m_0 to m_1 by a differentiable path Γ, with points m_t, and give an isometry ϕ_0 from $S^1 = \{|z| = 1\}$ to C^0 such that $z = 1$ is mapped onto the unit tangent to the curve Γ. Extend the isometry continuously to $\phi_t\colon S^1 \rightarrow C^t$ (C^t the unit tangent circle at m_t) so that for each t, $z = 1$ is mapped onto the tangent to Γ at m_t. Then $F(\phi_t)$ is a homotopy of $F(\phi_0)$ to $F(\phi_1)$, so that F has non-zero degree on C^1. Now for each $m \in M$ orient the tangent circle at m so that the degree of F restricted to this circle is positive. This gives a continuous orientation to M, which is impossible if M is not orientable.

In the remaining cases M is orientable, but not the torus, so the Euler characteristic $\chi(M)$ is not zero. We rely on this fact to show that the degree of the restriction of F to any tangent circle is zero.

Suppose this is not the case, and M is oriented so that the degree of F restricted to any tangent circle is $n > 0$. Then from F we can construct a continuous function F_0 on the tangent circle bundle so that on each circle it looks like $e^{i\alpha}z^n$. For this represent the circle bundle locally as pairs (m, θ), $m \in M$, $0 \leqq \theta < 2\pi$, so that θ is the arc length on the unit circle in the tangent plane at m, measured in the positive direction from some particular point on the circle. This representation is unique except for the choice of the point corresponding to $\theta = 0$. Where the representation is valid we have $F(m, \theta) = \exp i[n\theta + f(m, \theta)]$, with $f(m, \theta)$ continuous, of period 2π in θ, and determined $\bmod 2\pi$. Let $F_0(m, \theta) = \exp i[n\theta + \frac{1}{2\pi}\int_0^{2\pi} f(\theta)\, d\theta]$. Since f was determined $\bmod 2\pi$, $F_0(m, \theta)$ is well defined for this local representation of the tangent circle bundle. It is not difficult to check that F_0 is in fact independent of this representation, provided θ is the arc length from some point. Clearly F_0 is continuous. On each tangent circle F_0 assumes the value 1 at each of n equally spaced tangents, yielding what might be called a continuous spoke field over M. In the case $n = 2$ it is essentially a line element field over M. We show such a field cannot exist when $\chi(M) \neq 0$ by a device suggested by the article of L. Markus [2], basically the construction of a Riemann surface for a multiple-valued vector field.

Cover M with simply connected coordinate neighborhoods U_i with coordinates $x^i\colon U_i \to E_2$. On each U_i define n distinct cross sections $e_{i1}, \cdots, e_{in}$ of the tangent circle bundle such that $F_0(e_{ik}) = 1$. Consider $M^* = \{(m, e);$ $m \in M$, e in the tangent circle at m, and $F_0(e) = 1\}$. Let $U_{ik} = \{(m, e_{ik}(m));$ $m \in U_i\}$, and note that $(m, e) \in U_{ik}$ implies $e = e_{ik}(m)$. In U_{ik} define coordinates $x^{ik}\colon (m, e_{ik}(m)) \to x^i(m)$. We show that this makes M^* a manifold by checking the Jacobian of coordinate changes. For this consider (m_0, e_0) in $U_{ik} \cap U_{jl}$. Since $e_{ik}(m_0) = e_0 = e_{jl}(m_0)$, $e_{ik} = e_{jl}$ in a neighborhood U, with $m_0 \in U \subset U_i \cap U_j$. Let U' be the points (m, e) in $U_{ik} \cap U_{jl}$ for which $m \in U$. Then in U' $x^{ik}(m, e) = x^{ik}(m, e_{ik}(m)) = x^i(m)$, and similarly $x^{jl}(m, e) = x^j(m)$. Thus U' is mapped 1-1 onto an open subset of E_2 by x^{ik}, as well as by x^{jl}, and the Jacobian of the associated transformation of E_2 is the same as for x^i and x^j. Thus M^* is a manifold of the same class as M, except that M^* may not be connected. It forms an n-fold covering space for M with the projection $p\colon (m, e) \to m$. M^* also carries a non-zero vector field: to define it in U_{ik} we need only lift e_{ik} from U_i with the mapping of tangent spaces induced by the restriction of p to U_{ik}. This definition is easily shown to be consistent in $U_{ik} \cap U_{jl}$ by an argument like the one used above for the Jacobian. The Euler number of M^* is n times that of M; for any triangulation of M yields, by way of p^{-1}, a triangulation of M^* such that each simplex of M corresponds to n simplexes of M^*. Thus the Euler number of at least one of the components of M^* is not zero, contradicting the fact that each component carries a continuous non-zero vector field.

4. On the torus it is possible for an elliptic $C_\beta{}^\infty$ function on the circle bundle to have any degree. The approach here is to construct invertible $C_\beta{}^\infty$ operators with symbols of arbitrary degree. Consider the flat torus, i. e. the plane reduced 2π in both coordinates. Then any function in L^1 is represented by a double Fourier series, $f \sim \sum a_{nm} \exp i[nx_1 + mx_2]$. Let P_0 be projection on the constants, $P_0 f = a_{00}$. Let Δ be the Laplacian $(\partial/\partial x_1)^2 + (\partial/\partial x_2)^2$, and define $B = (P_0 - \Delta)^{-\frac{1}{2}}$. If f has Fourier coefficients a_{nm}, Bf has coefficients $b_{nm} = a_{nm}(n^2 + m^2)^{-\frac{1}{2}}$ $(n^2 + m^2 \neq 0)$, $b_{00} = a_{00}$. We want to show that $R_i = (\partial/\partial x_i)B$ is a $C_\infty{}^\infty$ operator ($C_\beta{}^\infty$ for every $\beta > 0$). For this an altered version of the proof given in [4] for the operator $(\partial/\partial x_i)J$ suffices. We give only the outline.

B is analyzed as a contour integral of the operators $F_\lambda = (\Delta - P_0 - \lambda)^{-1}$. The first step is to use the same approximation e_λ to f_λ as in [4], but let $K_\lambda = (\Delta - P_0 - \lambda)e_\lambda$. Then there is a real number L such that, for $\lambda \geqq L$, F_λ is given by the series $e_\lambda(1 + \sum_{m=1}^{\infty} (-1)^m K_\lambda{}^{(m)})$, which converges uniformly as a series of operators or as a series of kernels. We can now define F_λ for $0 \leqq \lambda < L$ by giving its kernel as a solution of

$$F_\lambda + LF_{L+\lambda}F_\lambda = F_{L+\lambda}. \tag{1}$$

This is possible, and uniquely, since $f \neq 0$ and $f + LF_{L+\lambda}f = 0$ would imply that $-1/L$ is in the spectrum of $F_{L+\lambda} = (\Delta - P_0 - L - \lambda)^{-1}$, contradicting the fact that this spectrum lies strictly between $-1/(L + \lambda)$ and zero. This is the proper extension of the F_λ, since for $\lambda < L$,

$$(\Delta - P_0 - \lambda)F_\lambda = [(\Delta - P_0 - L - \lambda) + L]F_{L+\lambda}(I - LF_\lambda) = I.$$

From its defining equation (1), F_λ has, for all λ, the same singularity as $F_{L+\lambda}$. The kernel for $(P_0 - \Delta)^{-\frac{1}{2}} = B$ is then given by a contour integral of the F_λ, from which it can be deduced as in [4], Theorem 5, that the kernel for B has a singularity $-(2/\pi^{\frac{1}{2}})r(x,y)^{-1}$, and that $R_i = (\partial/\partial x_i)J$ is a $C_\beta{}^\infty$ operator with symbol $-(-1)^{\frac{1}{2}}z_i/|z|$. Here we represent the cotangent bundle as (x, z) with $x = (x_1, x_2) \bmod 2\pi$, $z = (z_1, z_2)$; and let $|z|^2 = z_1{}^2 + z_2{}^2$. Since P_0 is completely continuous and smoothing of all orders, $U = P_0 + iR_1 - R_2$ is a $C_\beta{}^\infty$ operator with symbol $(z_1 + iz_2)/|z|$. Its action on the Fourier series shows that $UU^* = I$. Thus U and its inverse U^* are $C_\infty{}^\infty$ operators, and U is invertible on all L^p, $1 < p < \infty$.

This construction shows that $G_0 = (z_1 + iz_2)/|z|$ is in the class P of symbols of invertible $C_\beta{}^\infty$ operators. Suppose now we are given a symbol $G(x, z)$ such that its restriction to each cotangent circle is of degree n. Then $G_0{}^{-n}G$ has degree zero on each circle, and by Lemma 3 is in P. Thus $G = G_0{}^n(G_0{}^{-n}G)$ is also in P.

This completes the proof of Theorem 1.

5. Here we give results of Fredholm type, and on the smoothness of solutions of elliptic singular integral equations, which apply on a compact manifold M. We shall consistently assume that the numbers p, p_0, and q used below lie strictly between 1 and ∞. The discussion involves a few more of the ideas in [4], which we summarize. The space $L_{-n}{}^p$ $(n \geqq 0)$ is the set of bounded linear functionals on $L_n{}^q$, where $q^{-1} + p^{-1} = 1$. (There is a misprint in the corresponding convention given in [4]; page 672, line 15, should have $L_r{}^q$, not $L_r{}^p$.) If $\beta > 1$, any $C_\beta{}^\infty$ operator H can be considered as a bounded operator on $L_{-n}{}^p$ if $n \leqq \beta$, for H^* is a $C^{\beta\infty}$ operator, and hence bounded on $L_n{}^q$. With this notation, the definition of *smoothing of order n* given in Section 1 can be phrased as follows: an operator T is smoothing of order n if T and its adjoint preserve $L_m{}^p$ for $0 \leqq m \leqq n$, and T is bounded from $L_m{}^p$ to $L_{m+1}{}^p$ for $-n \leqq m < n$.

THEOREM 2. *Suppose H is an elliptic $C_\beta{}^\infty$ operator $(\beta \neq 1)$, $f \in L_m{}^p$, $g \in L_n{}^p$ $(-[\beta] \leqq m < n \leqq [\beta])$, and $Hf = g$. Then $f \in L_n{}^p$.*

Proof. Let H' be any $C_\beta{}^\infty$ operator with $\sigma(H') = \sigma(H)^{-1}$. Since $\sigma(H'H) = 1$, $H'H = I + K$, where I is the identity and K is smoothing of order n. From $Hf = g$ we conclude $f = H'g - Kf$. Here $Kf \in L_{m+1}{}^p$ and $H'g \in L_n{}^p$ so that, since $m < n$, we can conclude that $f \in L_{m+1}{}^p$. This argument can be repeated until we have $f \in L_n{}^p$.

THEOREM 3. *Let H be an elliptic $C_\beta{}^\infty$ operator, considered as an operator on some L^p, $1 < p < \infty$, and let H^* be its adjoint, an operator on L^q. Then*

i) *the nullities of H and H^* are finite and equal;*

ii) *the range of H is the orthogonal complement of the null space of H^*.*

Proof. (i) Let H' be a $C_\beta{}^\infty$ operator, invertible on L^p, with $\sigma(H') = \sigma(H)^{-1}$, so that $H'H = I + K$ with K completely continuous. Then, writing $\nu(A)$ for the dimension of the null space of A, $\nu(H) = \nu(H'H)$

$= \nu(H^*H'^*) = \nu(H^*)$. The second equality here is the standard result that $\nu(I+K) = \nu(I+K^*)$ for completely continuous K. It is also standard that $\nu(I+K)$ is finite.

(ii) We say $f \in L^p$ is orthogonal to $g \in L^q$ when $\int_M fg^*\,dv = 0$, and denote the orthogonal complement of a set S in L^p or L^q by $S^\perp$. Let N be the null space of H^* and R the range of H. Then it is trivial that $R \subset N^\perp$ and $R^\perp \subset N$. Since N is a closed linear subspace of L^q, $N^{\perp\perp} = N$; thus we find by taking further annihilators of the above inclusions that (closure of R) $= R^{\perp\perp} = N^\perp$. It remains to prove that R is closed. To do this, let H' be any $C_\beta{}^\infty$ operator with $\sigma(H'H) = 1$, so that $H'H = I + K$. Then as in the proof of (i) we deduce that N is finite dimensional, so that it has a closed linear complement L in L^p; i.e. L^p is the direct sum of N and L. For any g in R there is a unique f in L with $Hf = g$. Moreover there is a constant A such that, for all such g and f, $\| f \| \leqq A \| g \|$. To see this, suppose the contrary, i.e., suppose there is a sequence f_n with $\| f_n \| = 1$ and $Hf_n \to 0$. Then $H'Hf_n = f_n + Kf_n \to 0$. Since K is completely continuous, we can assume that Kf_n converges, so that f_n converges to some function f_0. Since L is closed, $f_0 \in L$; since $Hf_n \to 0$, $Hf_0 = 0$, and $f_0 = 0$, which contradicts $\| f_n \| = 1$. Thus $\| f \| \leqq A \| g \|$. Now let $g_n \in R$ and $g_n \to g$. Pick f_n in L with $Hf_n = g_n$. Then f_n is a bounded sequence. Pick a subsequence f'_n such that Kf'_n converges, and let $g'_n = Hf'_n$. Then $H'Hf'_n = f'_n + Kf'_n = H'g'_n \to H'g$, so that f'_n converges to an element f in L. Clearly $Hf = g$. Thus R, the range of H, is closed.

This completes the proof of Theorem 3. Part (ii) is practically the same as a proof given in Mihlin for L^2 ([3], pp. 33-34), and does not require Theorem 1. Theorem 2 does not require Theorem 1 either.

COROLLARY. *If $f \in L^{p_0}$ for some p_0, H is an elliptic $C_\beta{}^\infty$ operator, $Hf = g$, and $g \in L^p$ for all p, then $f \in L^p$ for all p.*

Proof. Let $S(p)$ be the set of functions ϕ in L^p satisfying $H\phi = g$. $S(p)$ is a coset in L^p of finite dimension $\nu(p)$. Since $L^p \supset L^{p'}$ for $p \leqq p'$, $\nu(p)$ is a non-increasing function of p. But $\nu(p) =$ dimension of null-space of H on $L^p =$ dimension of null-space of H^* on L^q $(q = p/(p-1))$, which is a non-decreasing function of p. Thus $\nu(p)$ is constant, and $S(p)$ is independent of p, so that the solutions in L^{p_0} are the same as those in L^p.

THEOREM 4. *Suppose H is an elliptic $C_\beta{}^\infty$ operator, $\beta > 1$, $f \in L_m{}^{p_0}$, $Hf = g$, and for all p, $g \in L_n{}^p$, with $n \geqq 0$, and $-[\beta] \leqq m < n \leqq [\beta]$. Then*

$f \in L_n^p$ for all p. If $n \geqq 1$, then f is of class $n-1$, i.e. f has continuous partial derivatives of order $n-1$.

Proof. By Theorem 2, $f \in L^{p_0}$. By the corollary above, $f \in L^p$ for all p. By Theorem 2 again, $f \in L_n^p$ for all p. In case $n \geqq 1$, a Sobolev lemma shows that f is of class $n-1$.

Remark. Theorem 3 could be proved for L_n^p in place of L^p, with a little more attention to the nature of C_β^∞ operators with vanishing symbol. Then the restriction to $n \geqq 0$ for the first conclusion in Theorem 4 could be removed.

HARVEY MUDD COLLEGE.

REFERENCES.

[1] A. P. Calderon and A. Zygmund, "Singular integral operators and differential equations," *American Journal of Mathematics*, vol. 79 (1957), pp. 901-921.

[2] L. Markus, "Line element fields and Lorentz structures on differentiable manifolds," *Annals of Mathematics*, sec. 2, vol. 62 (1955), pp. 411-417.

[3] S. G. Mihlin, "Singular integral equations," *American Mathematical Society Translation* number 24, 1950.

[4] R. T. Seeley, "Singular integrals on compact manifolds," *American Journal of Mathematics*, vol. 81 (1959), pp. 658-690.

[5] N. Steenrod, *The Topology of Fibre Bundles*, Princeton, 1951.

BIEBERBACH'S THEOREM ON SPACE GROUPS AND DISCRETE UNIFORM SUBGROUPS OF LIE GROUPS, II.*

By LOUIS AUSLANDER.[1]

Introduction. In the previous paper [1], with essentially the above title and henceforth called I, we discussed generalizations of the classical Bieberbach theorems. Our main result, listed as Theorem 1 in I was the following: Let N be a connected, simply connected nilpotent Lie group and let C be any compact Lie group of automorphisms of N. Further, let Γ be a discrete uniform subgroup of $N\cdot C$, where the dote denotes the semi-direct product. Then $\Gamma\cap N$ is uniform in N (H is uniform in G if G/H is compact) and $\Gamma/\Gamma\cap N$ is a finite group. At the end of I, we gave an example to show that the above result is false if N is replaced by a connected, simply connected solvable Lie group. It is the purpose of this paper to generalize the above result in two directions. Our main tool theorem is the following:

THEOREM 1. *Let S be a connected, simply connected solvable Lie group and let C be a compact group of automorphisms of S. Further, let Γ be a discrete (not necessarily uniform) subgroup of $S\cdot C$ and let $\overline{\Gamma S}$ be the closure of the group generated by the elements of Γ and S. Then the identity component of $\overline{\Gamma S}$ is solvable.*

From this we can deduce the following two results.

THEOREM 2. *Let Γ be a discrete uniform subgroup of $S\cdot C$, where S, C and $S\cdot C$ are as above. Then there exists a subgroup Γ^* of finite index in Γ such that Γ^* is a discrete uniform subgroup of a connected simply connected solvable Lie group S^*, where* $\dim. S = \dim. S^*$.

THEOREM 3. *Let Γ be a discrete subgroup of $N\cdot C$, where N is a connected, simply connected nilpotent Lie group, C is a compact group of automorphisms of N and the dot denotes the semi-direct product. Then there exists a subgroup Γ^* of finite index in Γ and a connected subgroup N^* of N such that Γ^* is a uniform subgroup of N^*.*

---

* Received December 9, 1960.

[1] Research supported by N. S. F. Grant 15565 and O. O. R. contract S A R-DA-19-020-ORD-5254.

Before proving our results a general word about method of proof may be in order. In I, we essentially used the same outline of proof as originally used by Bieberbach. In this paper, this is no longer the case. This paper indeed contains a new proof of the main theorem in I and can be read without reference to the results in I.

1. Proof of Theorem 1.

LEMMA 1. *Let $O(n)$ denote the orthogonal group and let $\gamma, \eta \in O(n)$. Then there is a neighborhood U of the identity in $O(n)$ such that if $\gamma, \eta \in U$ and $\gamma\eta \neq \eta\gamma$, then γ will not commute with $\gamma\eta\gamma^{-1}\eta^{-1} = (\gamma, \eta)$.*

Proof. Let us assume that γ and (γ, η) commute. Then γ and $\eta\gamma^{-1}\eta^{-1}$ commute. Hence η can be represented as a permutation of the invariant space of γ^{-1} or γ amongst themselves followed by a mapping of these spaces onto themselves. Hence if η is sufficiently close to the identity η can only map these invariant spaces onto themselves. Hence η and γ commute. This contradiction proves the lemma.

LEMMA 2. *Let G be a Lie group. Then there is a neighborhood W of the identity in G such that for any $g_1, g_2 \in W$, $(g_1, g_2) \in W$.*

Proof. Take canonical coordinates. The coordinates of (x, y) can be represented as power series in the coordinates of x and y with quadratic leading terms.

LEMMA 3. *Let $S \cdot C$ be as in Theorem 1 and let A be any normal, connected, simply connected abelian subgroup of $S \cdot C$. Assume that there exist elements in D whose images in $S \cdot C/A$ are arbitrarily close to the identity and, further, in the image of these elements in $S \cdot C/S$, there are elements arbitrarily close to the identity which do not commute. Then D is not discrete.*

Proof. Choose $\gamma_1, \gamma_2 \in D$ such that

1. The images of γ_1 and γ_2 in $S \cdot C/A$ satisfy the hypothesis of Lemma 2 with G replaced by $S \cdot C/A$.

2. The images of γ_1 and γ_2 in C satisfy the hypothesis of Lemma 1. Then choose $\gamma_i = x_i y_i$ such that $y_i \in A$ and x_i satisfies the hypothesis of Lemma 2 for $G = S \cdot C$. This is possible by the standard Lie group theory concerning existence of local cross-sections. Then

$$(\gamma_1, \gamma_2) = (x_1, x_2)\,\mathrm{ad}(x_1^{-1}x_2^{-1})\,[(\mathrm{ad}(x_2) - I)y_1 + (I - \mathrm{ad}(x_1))(y_2)],$$

where $\mathrm{ad}(x)$ denotes the automorphism of A induced by $x^{-1}Ax$. We may now choose x_1 and x_2 so small that $|\mathrm{ad}(x_i) - I| < 10^{-1}$. If we now form the series $\gamma_1, (\gamma_1, \gamma_2), (\gamma_1(\gamma_1, \gamma_2)), \cdots$, the x_i components remain in a bounded neighborhood of the identity by Lemma 2 and the components in A are easily seen to be bounded. But by Lemma 1, this series can never become the identity element from some index on. Hence D is not discrete.

Proof of Theorem 1. Let us assume that the theorem is false. Then let the identity component of $\overline{\Gamma S}$ be denoted by G^*. Hence there exist in $\Gamma S/S$ elements arbitrarily close to the identity which do not commute. Let $S^2 = [S, S]$, where $[\ ,\ ]$ denotes the commutator subgroup of the group in the bracket, and let $S^k = [S^{k-1}, S^{k-1}]$, where $S^r = 1$. Consider the group G^*/S^2. We wish to apply Lemma 3 to this group. We let $C = G^*/S$ and $A = S = S/S^2$ and let $D = \Gamma/S^2$. Then Γ/S^2 is not discrete in G^*/S^2 and we may seek to apply Lemma 3 again, but this time to the group G^*/S^3. Again let $C = G^*/S$. Let $S = S/S^3$, $A = S^2/S^3$ and $D = \Gamma/S^3$. Again we see that the hypothesis to Lemma 3 is satisfied and Γ/S^3 is not discrete in G^*/S^3. For the k step of the induction let $D = G^*/S$, $S = S/S^{k+1}$, $A = S^k/S^{k+1}$ and $D = \Gamma/S^{k+1}$. Then again Lemma 3 tells us that Γ/S^{k+1} is not discrete. Hence at the $r - 1$ step of the induction we get $\Gamma/S^r = \Gamma$ is not disecrete. This contradiction proves Theorem 1.

Remark. It might be worth noting here that Lemma 3 in the special case where $S = A$ can be used to provide an elementary proof of the classical Bieberbach Theorem. For let $W \subset A$ be the subspace of A spanned by the pure translations of Γ. Then Γ induces an action on A/W; i. e. we have a homomorphism of Γ into the group of rigid motions of A/W such that the identification space of A/W is a compact manifold. Further, the image of Γ contains no pure translations. Since the identity component of $\overline{\Gamma A}$ is solvable, the identity component of $\overline{\Gamma A}/A$ is abelian and it is then easy to see the above is impossible. Hence Γ contains dim. A linearly independent translations and the identity component of $\overline{\Gamma A}$ must be A.

2. Proof of Theorem 2.

THEOREM 2. *Let* Γ *be a discrete uniform subgroup of* $S \cdot C$. *Then there exists a subgroup* Γ^* *of finite index in* Γ *such that* Γ^* *is the discrete uniform subgroup of the solvable Lie group* S^*.

Proof. Let G equal the identity component of $\overline{\Gamma S}$ and let $\Gamma^* = \Gamma \cap G$. Now, since G/S is a compact solvable group, $G/S = T$ is abelian and the commutator subgroup of G, (G, G), is contained in S. Let M denote the maximal analytic nilpotent normal subgroup of S and let M^* denote the maximal normal analytic nilpotent subgroup of G. Then since M is a characteristic subgroup of S, M is normal in G and hence $M \subset M^*$. Further, it is trivial to verify that $M^*/M = T^*$ is compact. Hence M^* is isomorphic to $M \cdot T^*$. Now T^* must act trivially on M. But since G/M is solvable and S/M is abelian, T^* must act trivially on S/M. Hence since T^* is compact, it acts trivially on S and it is, therefore, the trivial group. This shows that M is the maximal normal nilpotent analytic subgroup of G. But then $M \supset (G, G)$. Hence G/M is abelian and isomorphic to the direct sum of T and S/M.

By a theorem of Mostow's [4] ΓM is closed in G. Hence $\Gamma/M \cap \Gamma = \Gamma^*$ is a discrete uniform subgroup in $T \oplus S/M$, where $\oplus$ denotes the direct sum. But if $\dim. S/M = r$, this means that Γ^* is free abelian on r generators, say $z_1, \cdots, z_r$. Since the exponential mapping is onto in G/M, we may choose one parameter groups $P_1(t), \cdots, P_r(t)$ such that $P_i(1) = z_i$, $i = 1, \cdots, r$. Let S^* be the subgroup of G generated by $P_1(t), \cdots, P_r(t)$ and M. Clearly S^* satisfies the conclusions of our theorem.

3. Proof of Theorem 3.

THEOREM 3. *Let Γ be a discrete subgroup of $N \cdot C$, where N is a connected, simply connected nilpotent Lie group, C is a compact group of automorphisms of N and the dot denotes the semi-direct product. Then there exists a subgroup of Γ^* of finite index in Γ and a connected subgroup N^* of N such that Γ^* is a uniform subgroup of N^*.*

Proof. Consider the identity component G of ΓN and let $\Gamma^* = G \cap \Gamma$. By Theorem 1, G is solvable and since $G/N = T$ is compact, it is abelian. Let W be the analytic subgroup of N left point-wise fixed under T. Now let $\Gamma_1^* = \Gamma^* \cap N$. We assert that $\Gamma_1^* \subset W$. This follows from the fact that Γ_1^* is normal in Γ^* and the action of Γ^* on Γ_1^* coming from components in T must be unimodular. This means that no element can be close to the identity. But from the definition of G, we can conclude that Γ^* acts trivially on Γ_1^* or $\Gamma_1^* \subset W$.

We now assert that we may choose a semi-direct product representation for G such that for all $\gamma \in \Gamma_1^* \gamma = w \cdot c$, where $w \in W$ and $c \in C$. To see this, we choose $\gamma_0 \in \Gamma^*$ such that the subgroup of N left point-wise fixed is exactly W. Now applying the arguments in [2], we see that we can choose $n_0 \in N$ such that $n_0 N \cdot T n_0^{-1}$ will be the desired semi-direct product for the single element n_0. But now if $\gamma \in \Gamma^*$ did not have the desired form in this semidirect product representation, $\gamma_0\gamma\gamma_0^{-1}\gamma^{-1}N \cap \Gamma^*$ would not lie in W. This proves the assertion.

Hence we have imbedded Γ^* in $W \oplus T$, where W is a connected, simply connected nilpotent Lie group and T is a compact torus group. Since Γ^* is discrete in $N \cdot C$, $\Gamma^*/\Gamma^* \cap T \approx \Gamma^*$ and Γ^* is a discrete subgroup of the group W. Now Theorem 3 follows from the standard theorems on discrete subgroups of nilpotent Lie groups.

REFERENCES.

[1] L. Auslander, "Bieberbach's theorem on space groups and discrete uniform subgroups of Lie groups," *Annals of Mathematics*, vol. 71 (1960), pp. 579-590.

[2] ———, "A fixed point theorem for nilpotent Lie groups," *Proceedings of the American Mathematical Society*, vol. 9 (1958), pp. 822-823.

[3] L. Bieberbach, "Über die Bewegungsgruppen der Euklidischen Räume I," *Mathematische Annalen*, vol. 70 (1911), pp. 297-336.

[4] G. D. Mostow, "Factor spaces of solvable groups," *Annals of Mathematics*, vol. 60 (1954), pp. 1-27.

ORTHOGONALE GRUPPEN ÜBER LOKALEN RINGEN.*

Von WILHELM KLINGENBERG.

---

1. Resultate.

1.0. In einer früheren Note [5] hatten wir die Struktur der linearen Gruppen über einem lokalen Ring bestimmt. In der vorliegenden Arbeit setzen wir das Studium der klassischen Gruppen über einem lokalen Ring fort mit der Untersuchung der orthogonalen Gruppen.

Das Hauptergebnis (siehe Theorem 6 unten) ist eine vollständige Bestimmung der invarianten Untergruppen einer orthogonalen Gruppe vom nicht-kompakten Typ über einem lokalen Ring L der Charakteristik $\neq 2$. Abgesehen von einigen Ausnahmefällen in niedrigen Dimensionen, ergibt sich das Folgende: Die Menge der invarianten Untergruppen zerfällt in disjunkte Klassen $\mathcal{B}(J)$, die den Idealen J von L entsprechen. Jede Klasse hat, bezüglich der Inklusion, ein grösstes und ein kleinstes Element, die durch gewisse Kongruenzuntergruppen modulo J repräsentiert werden, und jede Gruppe, die zwischen den extremalen Elementen der Klasse $\mathcal{B}(J)$ liegt, gehört zu der Klasse $\mathcal{B}(J)$.

Von derselben Art ist die Verteilung der invarianten Untergruppen bei der Kommutatorgruppe der orthogonalen Gruppe; in diesem Falle enthält jede Klasse $\mathcal{B}(J)$ höchstens zwei Elemente, und dann hat das kleinere den Index 2 in dem grösseren.

Die Struktur der orthogonalen Gruppen über einem lokalen Ring ist also von derselben Art, wie die Struktur der linearen Gruppen über einem solchen Ring: Wir hatten in [5] gezeigt, dass auch für eine lineare Gruppe über einem lokalen Ring die invarianten Untergruppen in Klassen zerfallen, die den Idealen entsprechen, so dass jede Klasse ein grösstes und ein kleinstes Element enthält und jede Gruppe dazwischen zu der Klasse gehört. Man kann also erwarten, dass dieses die typische Verteilung der invarianten Untergruppen einer klassischen Gruppe über einem lokalen Ring ist.

Falls der lokale Ring L nur die Ideale L und 0 besitzt, d. h., falls L ein Körper ist, so erhalten wir die bekannten Ergebnisse von Dieudonné [3], [4] über die orthogonalen Gruppen über einem Körper.

---

* Received November 28, 1960.

1.1. *Grundlegende Definitionen.* Ein *lokaler Ring* L ist ein kommutativer Ring mit Eins und einem grössten Ideal $I \neq L$. $L^* = L - I$ ist eine Gruppe unter der Multiplikation. Das homomorphe Bild eines lokalen Ringes, wenn es nicht der Nullring ist, ist wieder ein lokaler Ring. L/I ist ein Körper.

Wir setzen voraus: $\operatorname{char} L/I \neq 2$.

Unter einem (*n-dimensionalen*) *Vektorraum über* L verstehen wir einen L-Modul isomorph zu L^n, $n \geqq 1$. Sei Φ eine symmetrische Bilinearform auf dem Vektorraum M. Φ bestimmt einen Homomorphismus $d_\Phi \colon M \to M^*$ von M in den dualen Raum M^*, vgl. Bourbaki [2]. Φ heisst *nichtentartet,* wenn d_Φ ein Isomorphismus ist.

Unter einem *metrischen Vektorraum* (*über dem lokalen Ring* L) verstehen wir einen Vektorraum über L, auf dem eine nichtentartete symmetrische Bilinearform Φ gegeben ist. Bezeichnung: V oder $V(L)$.

Sei V ein metrischer Vektorraum. Ein *Unterraum von* V, U, ist ein Untermodul von V, betrachtet als L-Modul, mit folgenden Eigenschaften: (i) U ist direkter Summand in V, (ii) $\operatorname{Kern}(d_\Phi \mid U)$ ist direkter Summand in V.

Hier und im folgenden bezeichnet $d_\Phi \mid U$ die durch die Einschränkung von Φ auf U erklärte lineare Abbildung $d_{\Phi|U}$ von U in den dualen Raum U^*, das heisst, für $(X, Y) \in U \times U$ ist $(d_\Phi \mid U)(X)(Y) = \Phi(X, Y)$.

Falls L ein Körper, so ist jeder Untermodul ein Unterraum. Sei U ein Unterraum. Der von $d_\Phi U \subset V^*$ annullierte Untermodul U^0 est wieder ein Unterraum; wir nennen ihn den *zu U orthogonalen Unterraum.* Es ist $\dim U + \dim U^0 = \dim V$ und $U^{00} = U$. Ein Unterraum U von V heisst *isotrop,* wenn $\operatorname{Kern}(d_\Phi \mid U) \neq 0$, und *totalisotrop,* wenn $\operatorname{Kern}(d_\Phi \mid U) = U$. Beispiele von nichtisotropen Unterräumen (das sind Unterräume U mit $\operatorname{Kern}(d_\Phi \mid U) = 0$) sind V und 0. 0 ist gleichzeitig totalisotrop.

Ein Vektor $X \in V$ heisst *nichtisotrop,* wenn der von X erzeugte Untermodul $\langle X \rangle$ ein nichtisotroper Unterraum $\neq 0$ ist. X heisst isotrop, wenn $\langle X \rangle$ ein isotroper Unterraum ist. Ein nichtisotroper Vektor X ist gekennzeichnet durch $\Phi(X, X) \in L^*$. Ein isotroper Vektor X ist gekennzeichnet durch $X \neq 0$ modulo I und $\Phi(X, X) = 0$.

Seien V und V' metrisches Vektorräume. Ein Isomorphismus von V in V' heisst auch *Isometrie.*

Unter der *orthogonalen Gruppe von* V, $\boldsymbol{O}(V)$, verstehen wir die Gruppe der Isometrien von V auf sich. Die Isometrien mit Determinante 1 bilden die *spezielle orthogonale Gruppe von* V, $\boldsymbol{SO}(V)$.

1.2. *Die Theoreme von Witt und Cartan-Dieudonné.* Ein erstes wichtiges Ergebnis ist die Übertragung des Theorems von Witt auf metrische Vektorräume über einem lokalen Ring:

THEOREM 1. *Seien V und V' metrische Vektorräume über einem lokalen Ring. Es gebe eine Isometrie von V auf V'. Wenn $\sigma\colon U \to V'$ eine Isometrie eines Unterraumes U von V in V' ist, so gibt es eine Isometrie von V auf V', die eine Fortsetzung von σ ist.*

Als eine der Folgerungen haben wir, dass je zwei maximale totalisotrope Unterräume von V dieselbe Dimension haben. Diese Dimension heisst der *Index von V*, $\operatorname{ind} V$. Es gilt $2 \operatorname{ind} V \leqq \dim V$.

Sei U ein nichtisotroper Unterraum. Dann ist $V = U \perp U^0$ (direkte Summe). Die *Symmetrie bezüglich U* ist die Isometrie σ von V, die gegeben ist durch $\sigma \mid U = 1$ und $\sigma \mid U^0 = -1$.

Besonderns wichtig sind die Symmetrien bezüglich (nichtisotroper) Hyperebenen (das sind Unterräume der Kodimension 1). In Verallgemeinerung eines Resultats von E. Cartan und Dieudonné gilt das

THEOREM 2. *Sei $n = \dim V \geqq 2$. Jedes Element $\sigma \in \boldsymbol{O}(V)$ ist das Produkt von höchstens $2n-2$ Symmetrien an Hyperebenen. Dann und nur dann, wenn $\sigma \in \boldsymbol{SO}(V)$, ist die Anzahl der Symmetrien gerade.*

1.3. *Die Kongruenzuntergruppen.* Sei J ein Ideal in L mit $J \subset I$. Der natürliche Homomorphismus $g_J\colon L \to L/J$ bestimmt einen natürlichen *Homomorphismus* (den wir wiederum mit g_J bezeichnen)

$$g_J\colon V(L) \to V(L/J) \tag{1}$$

von $V = V(L)$ auf den metrischen Vektorraum $V(L/J)$ über dem lokalen Ring L/J, dessen nichtentartete symmetrische Bilinearform Φ_J festgelegt ist durch die Identität $\Phi_J(g_J X, g_J Y) = g_J \Phi(X, Y)$ für $(X, Y) \in V \times V$. Wir erklären $V(L/L)$ als 0-Modul und lassen in (1) jetzt auch das Ideal $J = L$ zu.

Der Homomorphismus g_J, (1), bestimmt einen *Homomorphismus*

$$h_J\colon \boldsymbol{O}(V(L)) \to \boldsymbol{O}(V(L/J)) \tag{2}$$

durch die Festsetzung $h_J \sigma g_J = g_J \sigma$ für $\sigma \in \boldsymbol{O}(V)$. Hier soll $\boldsymbol{O}(V(L/L))$ die Einheitsgruppe E sein. Ebenso setzen wir $\boldsymbol{SO}(V(L/L)) = E$.

Wenn wir absehen von den Fällen, dass $g_I V = V(L/I)$ die hyperbolische Ebene (d.h., $\dim g_I V = 2$, $\operatorname{ind} g_I V = 1$) über dem Körper $L/I = \boldsymbol{F}_3$ ist, dann ist Zentrum $\mathbf{O}(V) = \{1, -1\}$, wo 1 die Identität ist und -1 die Symmetrie am Unterraum 0.

Sei J ein Ideal in L. Unter der *Kongruenzgruppe* mod J *von* V, $\mathbf{O}(V, J)$, verstehen wir die invariante Untergruppe von $\mathbf{O}(V)$, die aus den Elementen $\sigma \in \mathbf{O}(V)$ besteht mit $h_J\sigma \in$ Zentrum $\mathbf{O}(g_J V)$. Unter der *speziellen Kongruenzuntergruppe* mod J *von* V, $\mathbf{SO}(V, J)$, verstehen wir die Gruppe $\mathbf{SO}(V) \cap \mathbf{O}(V, J)$.

Wenn $g_I V$ nicht die hyperbolische Ebene über $L/I = \mathbf{F}_3$ ist, so besteht $\mathbf{O}(V, J)$, für $J \subset I$, aus den $\sigma \in \mathbf{O}(V)$ mit $h_J\sigma = 1$ oder -1. Insbesondere ist $\mathbf{O}(V, L) = \mathbf{O}(V)$, $\mathbf{O}(V, 0) =$ Zentrum $\mathbf{O}(V)$, $\mathbf{SO}(V, L) = \mathbf{SO}(V)$, $\mathbf{SO}(V, 0) = \mathbf{SO}(V) \cap$ Zentrum $\mathbf{O}(V)$.

Sei J ein Ideal von L. Unter der *Kongruenz-Kommutatorgruppe* mod J *von* V, $\Omega(V, J)$, verstehen wir die gemischte Kommutatorgruppe von $\mathbf{O}(V)$ und $\mathbf{O}(V, J)$. Für $\Omega(V, L)$, d.h., für die Kommutatorgruppe von $\mathbf{O}(V)$, schreiben wir auch $\Omega(V)$. Wir erklären $\Omega(V(L/L))$ durch E.

Eine erste Kennzeichnung der Kongruenz-Kommutatorgruppen liefert das

THEOREM 3. *Sei* $\dim V \geqq 3$. *Sei* J *ein Ideal in* L.

(i) $\Omega(V, J)$ *ist die gemischte Kommutatorgruppe von* $\mathbf{SO}(V)$ *und* $\mathbf{SO}(V, J)$.

(ii) $\Omega(V, J)$ *wird erzeugt von den Elementen* $(\tau\tau')^2$, *wo* τ *und* τ' *Symmetrien an Hyperebenen sind und* $h_J(\tau\tau') = 1$.

Zu den Folgerungen aus diesem Theorem gehört, für $\dim V \geqq 3$: $\mathbf{SO}(V)/\Omega(V)$ ist kommutativ und jedes Element hat eine Ordnung $\leqq 2$. Zentralisator $\mathbf{SO}(V) =$ Zentralisator $\Omega(V) = \{1, -1\}$, also Zentrum $\mathbf{SO}(V) = \mathbf{SO}(V) \cap \{1, -1\}$, Zentrum $\Omega(V) = \Omega(V) \cap \{1, -1\}$. Für ein Ideal $J \subset I$ ist $\mathbf{SO}(V, J) = h_J^{-1}$ Zentrum $\mathbf{SO}(g_J V)$.

1.4. *Die Cliffordalgebra. Eine zweite Charakterisierung der Kongruenz-Kommutatorgruppen mit Hilfe der Spinornorm für* ind $V \geqq 1$. Die *Cliffordalgebra über* V, $C(V)$, ist in der üblichen Weise erklärt, vgl. Bourbaki [2]. $C^+(V)$ bezeichne die Unteralgebra, die erzeugt wird von den Produkten aus einer geraden Anzahl von Vektoren, aufgefasst als Elemente von $C(V)$. In der multiplikativen Gruppe von $C^+(V)$ haben wir die *spezielle Cliffordgruppe*, $D(V)$, bestehend aus den Produkten einer geraden Anzahl von nichtisotropen Vektoren.

$D(V)/L^*$ ist kanonisch isomorph zu $\mathbf{SO}(V)$. Dieser Isomorphismus induziert einen Homomorphismus $\theta\colon \boldsymbol{SO}(V) \to L^*/L^{*2}$, der *Spinornorm* heisst. Kern θ heisst *reduzierte orthogonale Gruppe*, $\boldsymbol{O}'(V)$.

Es ist $\Omega(V) \subset \boldsymbol{O}'(V)$. Falls $\operatorname{ind} V \geqq 1$, so fallen diese beiden Gruppen zusammen, und die Spinorum übernimmt für die orthogonalen Gruppen die Rolle, die Determinante für die linearen Gruppen spielt:

THEOREM 4. *Sei J ein Ideal in L mit $J \subset I$. Es bezeichne θ_J den Homomorphismus*

$$\theta \times h_J\colon \sigma \in \boldsymbol{SO}(V) \to (\theta(\sigma), h_J\sigma) \in L^*/L^{*2} \times \boldsymbol{SO}(g_J V).$$

(i) *Sei* $\dim V = 2$ *oder* $\operatorname{ind} V \geqq 1$. *Dann ist*
$$\operatorname{Kern}\theta = \Omega(V), \quad \operatorname{Kern}\theta_J = \Omega(V, J).$$

(ii) *Sei* $\operatorname{ind} V \geqq 1$. *Dann ist*
$\boldsymbol{SO}(V)/\Omega(V)$ *isomorph zu* $\operatorname{Bild}(\theta) = L^*/L^{*2}$.
Sei ausserdem $\dim V \geqq 3$. *Dann ist*
$\boldsymbol{SO}(V, J)/\Omega(V, J)$ *isomorph zu* Bild $(\theta_J \mid \boldsymbol{SO}(V, J)) =$ *Untergruppe der Paare* $(aL^{*2}, \bar{\sigma})$ *in* $L^*/L^{*2} \times \operatorname{Zentrum} \boldsymbol{SO}(g_J V)$ *mit* $g_J a L^{*2} = \theta(\bar{\sigma})$.

(iii) *Sei* $\dim V \geqq 3$, $\operatorname{ind} V \geqq 1$.
Dann ist $(\boldsymbol{SO}(V, J) \cap \Omega(V))/\Omega(V, J)$ *isomorph zu* Zentrum $\Omega(g_J V)$.

1.5. *Die Struktur der orthogonalen Gruppen für* $\dim V \leqq 4$. Die Cliffordalgebra $C(V)$ über V liefert, für $\dim V \leqq 4$, in natürlicher Weise Isomorphismen von Gruppen $\boldsymbol{SO}(V)$ in projektive lineare Gruppen in 2 Variablen. Diese Isomorphismen sind fundamental für die Bestimmung der Struktur orthogonaler Gruppen von beliebig dimensionalen Räumen, vgl. 1.6.

THEOREM 5.

(i) *Sei* $\dim V = 2$. (a) *Sei* $\operatorname{ind} V = \operatorname{ind} g_I V = 0$. *Dann ist* $\boldsymbol{SO}(V)$ *isomorph* L'^*/L^*, *wo* $L' = L((-\Delta)^{\frac{1}{2}})$ *ein lokaler Ring ist, der aus L durch quadratische Erweiterung mit einem Element* $-\Delta$, $\Delta \in \theta(-1)$, *entsteht.*
(b) *Sei* $\operatorname{ind} V = 1$. *Dann ist* $\boldsymbol{SO}(V)$ *isomorph* L^*.

(ii) *Sei* $\dim V = 3$ *und* $\operatorname{ind} V = 1$. *Dann ist* $\boldsymbol{SO}(V)$ *isomorph zu* $PGL(2, L) = GL(2, L)/\operatorname{Zentrum} GL(2, L)$.

(iii) *Sei* $\dim V = 4$. (a) *Sei* $\operatorname{ind} V = \operatorname{ind} g_I V = 1$. *Dann ist* $\boldsymbol{PSO}(V) = \boldsymbol{SO}(V)/\operatorname{Zentrum} \boldsymbol{SO}(V)$ *isomorph zu einer Untergruppe von*

$PGL(2,L')$, die $PSL(2,L')$ umfasst, wobei $L' = L(\Delta^{\frac{1}{2}})$ ein lokaler Ring ist, der aus L durch quadratische Erweiterung mit einem Element $\Delta \in \theta(-1)$ entsteht.

(b) *Sei* $\operatorname{ind} V = 2$. *Dann ist* $P\Omega(V) = \Omega(V)/\text{Zentrum}\,\Omega(V)$ *isomorph zu* $PSL(2,L) \times PSL(2,L)$.

1.6. *Die Struktur der Gruppen* $\mathbf{SO}(V)$ *und* $\Omega(V)$ *für* $\operatorname{ind} V \geqq 1$ *und* $\dim V \geqq 3$. Sei $\sigma \in \mathbf{O}(V)$. Unter der *Ordnung von* σ, $o(\sigma)$, verstehen wir das kleinste Ideal J in L so, dass $\sigma \in \mathbf{O}(V,J)$.

Sei G eine Untergruppe von $\mathbf{O}(V)$. Unter der *Ordnung von* G, $o(G)$, verstehen wir das kleinste Ideal J so, dass $\mathbf{O}(V,J) \supset G$, das heisst, $h_J G \subset \text{Zentrum}\,\mathbf{O}(g_J V)$.

Offenbar wird $o(G)$ erzeugt von den Idealen $o(\sigma)$, wo σ die Elemente von G durchläuft.

Sei $\dim V \geqq 3$. Aus Theorem 3 folgt, dass $\Omega(V,J)$ die Ordnung J hat. Theorem 4(ii) lehrt, dass $\mathbf{SO}(V,J)/\Omega(V,J)$ kommutativ ist, und da $\Omega(V,J)$ invariant ist ergibt sich: Jede Untergruppe G von $\mathbf{SO}(V)$ mit $\Omega(V,J) \subset G \subset \mathbf{SO}(V,J)$ ist invariant und von der Ordnung J. Unser Hauptergebnis ist, dass dieses auch die einzigen invarianten (ja sogar die einzigen unter $\Omega(V)$ invarianten) Untergruppen der Ordnung J von $\mathbf{SO}(V)$ sind:

THEOREM 6. *Sei* $\operatorname{ind} V \geqq 1$. *Sei* $\dim V \geqq 5$ *oder* $\dim V = 4$ *und* $\operatorname{ind} g_I V = 1$ *oder* $\dim V = 3$ *und* $L/I \neq \mathbf{F}_3$.

(i) *Jede Untergruppe G von $\mathbf{SO}(V)$ der Ordnung $o(G) = J$, die invariant ist unter $\Omega(V)$, genügt den Beziehungen*

$$\Omega(V,J) \subset G \subset \mathbf{SO}(V,J). \tag{3}$$

Andererseits ist jede Untergruppe G von $\mathbf{SO}(V)$, die den Beziehungen (3) genügt, invariant und von der Ordnung J.

(ii) *Eine invariante Untergruppe von $\Omega(V)$ der Ordnung J ist von der Form $\mathbf{SO}(V,J) \cap \Omega(V)$ oder $\Omega(V,J)$.*

KOROLLAR. (Dieudonné [3], [4]) *Sei L ein Körper. Unter den angegebenen Voraussetzungen gilt*

(i) *Eine Untergruppe G von $\mathbf{SO}(V)$, die invariant ist unter $\Omega(V)$, genügt einer beiden Beziehungen*

$$E \subset G \subset \text{Zentrum}\,\mathbf{SO}(V), \qquad \Omega(V) \subset G \subset \mathbf{SO}(V).$$

Andererseits ist jede Untergruppe G von $\mathbf{SO}(V)$, die einer dieser Beziehungen genügt, invariant in $\mathbf{SO}(V)$.

(ii) *Die invarianten und echten Untergruppen von* $\Omega(V)$ *gehören zu* Zentrum $\Omega(V)$. $P\Omega(V)$ *ist einfach.*

1.7. *Bemerkung.* Die Beweise der vorstehenden Ergebnisse beruhen auf einer Weiterentwicklung und Verfeinerung der Methoden, die, zu einem wesentlichen Teil von Dieudonné, für die Untersuchung der orthogonalen Gruppen über einem Körper entwickelt worden sind.

Insbesondere wird Theorem 6 dadurch bewiesen, dass die Struktur von $\boldsymbol{SO}(V)$ in Verbindung gebracht wird mit der Struktur der in Theorem 5(ii) und (iii, a) genannten Gruppen, also mit projektiven linearen Gruppen in 2 Variablen. Die Struktur dieser Gruppen hinwieder ergibt sich aus früheren Untersuchungen [5] von uns vgl. den Anhang.

Im übrigen schliessen wir uns in den Bezeichnungen und in den Beweisen soweit wie möglich der Darstellung an, die Artin [1] von der Theorie der orthogonalen Gruppen über einem Körper gegeben hat. Bei den einleitenden Abschnitten und bei der Einführung der Cliffordalgebra sei auch verwiesen auf Bourbaki [2].

2. Allgemeine Theorie der orthogonalen Gruppen. Theorem 1 und 2.

2.1. *Allgemeine Vereinbarungen.* Mit L bezeichen wir einen lokalen Ring mit grösstem Ideal $I \neq L$ und char $L/I \neq 2$.

Mit V oder auch $V(L)$ bezeichen wir einen metrischen Vektorraum über L. Die nichtentartete symmetrische Bilinearform von V werde mit Φ bezeichnet. Es bezeichne

$$d_\Phi : V \to V^* \tag{4}$$

den durch $d_\Phi X(Y) = \Phi(Y, X) = \Phi(X, Y)$ erklärten Isomorphismus von V, aufgefasst als freier L-Modul, in den dualen L-Modul V^*.

Seien $X, Y, Z, \cdots$. Elemente von V. Den von diesen Elementen erzeugten Untermodul bezeichnen wir mit $\langle X, Y, Z, \cdots\rangle$.

Für das *Skalarprodukt* $\Phi(X, Y)$ zweier Vektoren X und Y von V schreiben wir auch XY. X^2 steht für XX. Wenn $XY = 0$, so sagen wir auch: *X und Y sind orthogonal zueinander.*

Seien U, U_1 und U_2 Unterräume von V. Wir sagen: *U_1 und U_2 bilden eine orthogonale Zerlegung von U,* in Zeichen: $U = U_1 \perp U_2$, wenn U direkte Summe ist von U_1 und U_2 und wenn jeder Vektor von U_1 orthogonal ist zu jedem Vektor von U_2. Hier lassen wir auch ausdrücklich den Fall zu, dass $U_1 = 0$, der Nullraum, und $U_2 = U$ ist. Sei $V = U \perp W$ eine orthogonale Zerlegung von V. Wenn $\sigma : V \to V'$ eine Isometrie von V in den metrischen

Vektorraum V' ist, so ist σ eindeutig bestimmt durch die Restriktionen $\rho = \sigma \mid U : U \rightarrow V'$ und $\tau = \sigma \mid W : W \rightarrow V'$. Wir schreiben daher σ auch in der Form $\rho \perp \tau$.

Für die identische Abbildung von V auf sich, $X \rightarrow X$, schreiben wir auch 1, und für die Symmetrie an 0, $X \rightarrow -X$, schreiben wir auch -1.

Sei A ein nichtisotroper Vektor. Für die Symmetrie an dem zu $\langle A \rangle$ orthogonalen Raum $\langle A \rangle^0$ (vgl. Satz 1) schreiben wir auch τ_A.

2.2. *Orthogonalität.*

SATZ 1. *Sei U ein Unterraum von V. Bezeichne U^0 den von $d_\Phi U \subset V^*$ annullierten Untermodul von V. U^0 ist ein Unterraum und es gilt*

$$\dim U + \dim U^0 = \dim V. \tag{5}$$

Es ist $U^{00} = U$. Es ist

$$U \cap U^0 = \operatorname{Kern}(d_\Phi \mid U) = \operatorname{Kern}(d_\Phi \mid U^0) \tag{6}$$

$U \cap U^0$ ist totalisotrop.

Wenn W ein in U zu $U \cap U^0$ komplementärer Untermodul ist, so ist $\operatorname{Kern}(d_\Phi \mid W) = 0$, *das heisst, W ist ein nichtisotroper Unterraum, und es ist*

$$U = U \cap U^0 \perp W. \tag{7}$$

Beweis. Da d_Φ, (4), ein Isomorphismus ist, ist $d_\Phi U = U^*$ ein direkter Summand von V^*. Also ist auch der von U^* annullierte Untermodul U^0 von V direkter Summand und es gilt, wegen $\dim U = \dim U^*$, (5). Da $U^{00} \supset U$ und $\dim U^{00} = \dim U$, ist $U^{00} = U$.

Für $X \in U$ ist die Eigenschaft: "$d_\Phi X(Y) = \Phi(X, Y) = d_\Phi Y(X) = 0$ für alle $Y \in U$" gleichwertig mit "$X \in \operatorname{Kern}(d_\Phi \mid U)$" und gleichwertig mit "$X \in U^0$," also gilt die erste Gleichung in (6), und aus Symmetriegründen gilt auch die zweite. Das heisst insbesondere, dass Kern $(d_\Phi \mid U^0)$ ein direkter Summand ist, also U^0 ein Unterraum.

Da $\operatorname{Kern}(d_\Phi \mid U \cap U^0) = U \cap U^0$, ist $U \cap U^0$ totalisotrop.

Sei W komplementär zu $U \cap U^0$ in U. Für $X \in U \cap U^0$ und $Z \in W$ haben wir $XZ = d_\Phi X(Z) = 0$. Da $\operatorname{Kern}(d_\Phi \mid W) \subset \operatorname{Kern}(d_\Phi \mid U) = U \cap U^0$ und $W \cap U \cap U^0 = 0$, ist $\operatorname{Kern}(d_\Phi \mid W) = 0$, also gilt (7).

Bemerkung. Sei U ein Unterraum. $U \cap U^0$ heisst *Radikal von U*, rad U. U nichtisotrop ist gleichwertig mit rad $U = 0$.

SATZ 2. *Sei U ein Unterraum von V, U^0 der zu U orthogonale Unterraum. Folgende Eigenschaften sind äquivalent:*

(i) U *ist nichtisotrop,*

(ii) U^0 *ist nichtisotrop,*

(iii) $V = U \perp U^0$.

Beweis. Es gelte (i), das heisst, $d_\Phi \mid U$ sei ein Isomorphismus. Zu jedem $Y \in V$ gibt es genau ein $Y_0 \in U$ so, dass $d_\Phi Y \mid U = d_\Phi Y_0 \mid U$, das heisst, $Y - Y^0 \in U^0$, es gilt also (iii). (iii) impliziert (i), denn wenn $\mathrm{Kern}(d_\Phi \mid U) \neq 0$, so $U \cap U^0 \neq 0$ und wegen $U^{00} = U$ impliziert (iii) auch (ii) und (ii) impliziert wiederum (iii).

SATZ 3. *Sei U ein Unterraum von V so, dass $X^2 = 0$ für jedes $X \in U$. Dann ist U totalisotrop.*

Beweis. $XY = ((X+Y)^2 - X^2 - Y^2)/2 = 0$ für beliebige X und Y aus U.

SATZ 4. *V besitzt eine orthogonale Basis, d.h., es gibt eine Basis E_i, $1 \leq i \leq n = \dim V$, von V so, dass die E_i nichtisotrop sind und $E_iE_k = 0$ für $i \neq k$.*

Beweis. Da V nichtisotrop ist, gibt es in V einen nichtisotropen Vektor E_1 (wir setzen stets $\dim V > 0$ voraus). Wenn $\dim V > 1$, so folgt aus Satz 2, dass $\langle E_1\rangle^0 \neq 0$ und nichtisotrop ist und von der Dimension $n-1$. Der Beweis ergibt sich also durch Induktion.

2.3. *Die Witt-Zerlegung. Theorem* 1. Seien N und M zwei isotrope Vektoren in V mit $NM = 1$. Wir sagen dann: *N, M bilden ein hyperbolisches Paar.*

Sei N, M ein hyperbolisches Paar. Dann sind N und M modulo I linear unabhängig, das heisst, $\langle N, M\rangle$ ist ein direkter Summand. Da ferner $\mathrm{Kern}(d_\Phi \mid \langle N, M\rangle) = 0$, ist $\langle N, M\rangle$ sogar ein nichtisotroper Unterraum; wir bezeichnen ihn auch als *hyperbolische Ebene.*

Sei U ein nichtisotroper Unterraum. Unter einer *Witt-Zerlegung von U* verstehen wir eine direkte Zerlegung der Form

$$U = U' + U'' \perp W \tag{8}$$

wobei U' und U'' totalisotrope Räume sind und W nichtisotrop.

SATZ 5. *Sei P ein nichtisotroper, 2-dimensionaler Unterraum von V. Wenn N ein isotroper Vektor in P ist, so gibt es genau einen weiteren isotropen Vektor M in P mit $NM = 1$. Damit wird $P = \langle N, M\rangle$.*

Beweis. Da P nichtisotrop ist, gibt es $A \in P$ mit $NA \in L^*$. Wir setzen $M = Nx + Ay$ und bestimmen y aus $1 = NAy$ und x aus $0 = NA2xy + A^2y^2$.

SATZ 6. *Sei U ein Unterraum von V und sei U in der Form (7) zerlegt. Falls $U \cap U^0 \neq 0$, so sei $N_1, \cdots, N_r$ eine Basis des totalisotropen Raumes $U \cap U^0$. Dann gibt es isotrope Vektoren $M_1, \cdots, M_r$ in V so, dass N_j, M_j für jedes j, $1 \leqq j \leqq r$, ein hyperbolisches Paar bilden und so, dass die hyperbolischen Ebenen $P_j = \langle N_j, M_j\rangle$ paarweise orthogonal auch zu W orthogonal sind. Wir erklären den nichtistropen Raum $\bar{U}$ durch*

$$(9) \qquad \bar{U} = P_1 \perp \cdots \perp P_r \perp W = \langle N_1, \cdots, N_r\rangle + \langle M_1, \cdots, M_r\rangle \perp W.$$

Hier steht an der letzten Stelle eine Witt-Zerlegung von $\bar{U}$.

Beweis. Für $r = 0$ ist der Satz jedenfalls richtig. Sei $r \geqq 1$ und sei der Satz für $r - 1$ schon beweisen. Wir setzen $U_0 = \langle N_1, \cdots, N_{r-1}\rangle \perp W$. Dann ist $U_0{}^0 = U^0 \perp \langle N_r\rangle$, $\operatorname{rad} U_0 = \operatorname{rad} U_0{}^0 = \langle N_1, \cdots, N_{r-1}\rangle$. Wegen $\langle N_r\rangle^0 \cap U_0{}^0 = \langle N_r, U_0\rangle^0 = U^0$ gilt für einen Vektor $A \in U_0{}^0$ mit der Eigenschaft $U_0{}^0 = U^0 + \langle A\rangle$: $AN_r \in L^*$. Daher gibt es auch in $U_0{}^0$ ein hyperbolisches Paar der Form N_r, M_r. Mit $P_r = \langle N_r, M_r\rangle$ ist auch $P_r{}^0$ nichtisotrop, und es ist $U_0 \subset P_r{}^0$. Nach Induktionsvoraussetzung gibt es in dem nichtisotropen Raum $P_r{}^0$ einen Raum der Form $\bar{U}_0 = P_1 \perp \cdots \perp P_{r-1} \perp W$. Durch $\bar{U}_0 \perp P_r$ erklären wir dann $\bar{U}$.

SATZ 7. *Sei $\sigma: U \rightarrow V'$ eine Isometrie eines Unterraumes U von V in einen metrischen Vektorraum V'. Dann lässt σ sich erweitern auf den in Satz 6 erklärten, U unfassenden Unterraum $\bar{U}$, (9), von V.*

Beweis. Setze $\sigma N_i = N'_i$ und $\sigma W = W'$. Für $\sigma U = U'$ haben wir dann die Zerlegung $U' = \langle N'_1, \cdots, N'_r\rangle \perp W'$. Nach Satz 6 gibt es in V' eine Erweiterung von U' zu $\bar{U}'$ mit Hilfe von isotropen Vektoren $M'_1, \cdots, M'_r$. Wenn wir die $M_j \in \bar{U}$ abbilden auf die $M'_j \in \bar{U}'$, haben wir σ auf $\bar{U}$ erweitert.

THEOREM 1. *Seien V und V' metrische Vektorräume. Es gebe eine Isometrie von V auf V'. Wenn $\sigma: U \rightarrow V'$ eine Isometrie eines Unterraumes U von V in V' ist, so lässt σ sich erweitern zu einer Isometrie von V auf V'.*

Beweis. 1. Sei $\bar{U}$ eine Erweiterung von U zu einem nichtisotropen Raum, wie es sie nach Satz 6 gibt. Nach Satz 7 lässt σ sich jedenfalle auf $\bar{U}$ fortsetzen. Wir können daher von vorneherein annehmen, dass U nichtisotrop ist.

2. Angenommen, das Theorem ist für niedrigere Dimensionen schon

bewiesen. Wir schreiben U in der Form $U = U_1 \perp U_2$. Setze $\sigma U_1 = U'_1$ und $\sigma \mid U_1 = \tau$. Dann lässt τ sich auf V erweitern. $U_1{}^0$ geht dabei über in $U'_1{}^0$, insbesondere sind also $U_1{}^0$ und $U'_1{}^0$ isometrisch. $\sigma \mid U_2$ bildet U_2, das ja zu $U_1{}^0$ gehört, in $U'_1{}^0$ ab. Es gibt also eine Erweiterung von $\sigma \mid U_2$ zu einer Abbildung $\lambda\colon U_1{}^0 \to U'_1{}^0$. $\tau \perp \lambda\colon V = U_1 \perp U_1{}^0 \to U'_1 \perp U'_1{}^0 = V'$ ist die gesuchte Erweiterung.

3. Da ein nichtisotroper Unterraum U als orthogonale Summe von 1-dimensionalen nichtisotropen Unterräumen dargestellt werden kann (Satz 4), genügt es, das Theorem für den Fall $U = \langle A \rangle$, A nichtisotrop, zu beweisen. Sei $\sigma A = A'$. Sei $\rho\colon V \to V'$ eine Isometrie von V auf V'. Setze $\rho^{-1}A' = B$. Wenn wir eine Isometrie $\tau\colon V \to V$ mit $\tau A = B$ angeben, dann ist $\rho\tau\colon V \to V'$ eine Erweiterung von σ.

Wegen $(A + B)(A - B) = 0$ ist einer der Vektoren $A + B$ und $A - B$ nichtisotrop. Denn wären sowohl $g_I(A + B)$ als auch $g_I(A - B)$ isotrop, so wären auch g_IA und g_IB isotrop. Sei also $D = A + \epsilon B$, mit $\epsilon = 1$ oder -1, nichtisotrop. Sei $\tau = \tau_D$ die Symmetrie an $\langle D \rangle^0$. Dann ist $\tau A = -\epsilon B$ und $-1\tau A = \epsilon B$. τ oder -1τ ist also eine Isometrie von V, die A in B überführt.

Folgerung 1. *Je zwei maximale totalisotrope Unterräume von V sind isometrisch.*

Die Dimension eines solchen Raumes heisst *Index von* V, ind V.

Folgerung 2. *Ausgehend von einem maximalen totalisotropen Unterraum von V mit den Basiselementen $N_1, \cdots, N_r$, $r =$ ind V, ergeben sich auf Grund von Satz* 6 *r paarweise zueinander orthogonale hyperbolische Ebenen $H_1, \cdots, H_r$ in V. Den zu der Summe dieser Ebenen orthogonalen Raum bezeichnen wir mit W. Damit erhalten wir für V die Darstellung*

$$V = H_1 \perp \cdots \perp H_r \perp W \qquad r = \operatorname{ind} V, \operatorname{ind} W = 0. \tag{10}$$

Durch (10) *ist eine Witt-Zerlegung von V bestimmt, vgl.* (9).

Folgerung 3. *Sind U_1, U_2 isometrische Unterräume von V, so sind auch $U_1{}^0$, $U_2{}^0$ isometrisch.*

Ergänzung zu Theorem 1. *Sei $\sigma\colon U \to V$ eine Isometrie eines Unterraumes U von V in V. Falls* $\dim U + \dim \operatorname{rad} U < \dim V$, *so gibt es unter den Erweiterungen von σ zu einer Isometrie von V auf V solche, die zu $\mathbf{SO}(V)$ gehören, und solche, die nicht zu $\mathbf{SO}(V)$ gehören.*

Beweis. Die Voraussetzung bedeutet, dass der nach Satz 6 zu U gehörige Raum $\bar{U}$, (9), eine Dimension $< \dim V$ hat. Daher gibt es in $\bar{U}^0$ einen nichtisotropen Vektor A. Sei $\tau = \tau_A$. Wenn $\rho \colon V \to V$ eine Erweiterung von σ ist, so auch $\tau\rho$, und $\det \tau\rho = -\det \rho$.

2.4. *Das Zentrum von $\boldsymbol{O}(V)$.*

SATZ 8. *Sei* $\dim V \geqq 3$ *und* $\operatorname{ind} V \geqq 1$, *das heisst, V enthalte isotrope Geraden* ($=$ *1-dimensionale Unterräume*). *Sei $\sigma \in \boldsymbol{O}(V)$. Sei J ein Ideal von L so, dass für jede isotrope Gerade $\langle N \rangle$ gilt: $g_J\langle \sigma N \rangle = g_J\langle N \rangle$. Dann ist $h_J\sigma = \pm 1$.*

Beweis. Die Behauptung ist trivialerweise richtig für $J = L$. Wir nehmen daher an: $J \subset I$. V enthält ein hyperbolisches Paar N, M. Es sei $g_J\sigma N = h_J\sigma g_J N = g_J Na$ und $g_J\sigma M = h_J\sigma g_J M = g_J Mb$. $P^0 = \langle N, M \rangle^0$ ist nichtisotrop und besitzt eine Basis aus nichtisotropen Vektoren E. Wenn wir zeigen, dass für jeden dieser Vektoren E gilt: $g_J\sigma E = h_J\sigma g_J E = g_J Ec$ mit $g_J c = g_J a = g_J b$, so heisst das, dass $h_J\sigma$ eine Homothetie von $g_J V$ ist, und da $h_J\sigma \epsilon \boldsymbol{O}(g_J V)$, folgt die Behauptung.

Wir betrachten jetzt den nichtisotropen Raum $U = \langle N, M, E \rangle$. In U liegt der isotrope Vektor $N - ME^2/2 + E$. Nach Voraussetzung ist $g_J\sigma(N - ME^2/2 + E) = g_J(N - ME^2/2 + E)d = g_J Na - g_J MbE^2/2 + g_J\sigma E$. Hieraus folgt $g_J\sigma E \in g_J U$, und da $g_J\sigma E$ orthogonal ist zu $g_J\sigma P = g_J P$, folgt $g_J\sigma E = g_J Ec$ und damit $g_J a = g_J b = g_J c$.

SATZ 9. *Sei σ eine Isometrie, die alle nichtisotropen Geraden von V festlässt. Wenn dann $g_I V$ nicht die hyperbolische Ebene über dem Primkörper $L/I = \boldsymbol{F}_3$ ist, so folgt $\sigma = \pm 1$.*

Beweis. Wir wählen eine orthogonale Basis in V. Es seien A, B zwei verschiedene Elemente dieser orthogonalen Basis. Nach Voraussetzung haben wir $\sigma A = Aa$ und $\sigma B = Bb$. Wenn wir zeigen, dass $a = b$, so ist σ eine Homothetie, und da σ eine Isometrie ist, folgt $\sigma = \pm 1$.

Falls nicht $L/I = \boldsymbol{F}_3$ und gleichzeitig $g_I\langle A, B \rangle$ hyperbolisch ist, so gibt es in $\langle A, B \rangle$ eine nichtisotrope Gerade $\langle Au + Bv \rangle$, die modulo I verschieden ist von $\langle A \rangle$ und $\langle B \rangle$, d.h., $u \in L^*$ und $v \in L^*$; im Falle $L/I = \boldsymbol{F}_3$ ist es z.B. die Gerade $\langle A + B \rangle$. Aus $\sigma(Au + Bv) = (Au + Bv)d = Aau + Bbv$ folgt dann $a = b$.

Es bleibt der Fall zu betrachten: $L/I = \boldsymbol{F}_3$ und $g_I\langle A, B \rangle$ hyperbolisch. Nach Voraussetzung gibt es dann in $\langle A, B \rangle^0$ einen nichtisotropen Vektor C. $A + B + C$ ist nichtisotrop. Aus $\sigma(A + B + C) = (A + B + C)d = Aa + Bb + Cc$ folgt wiederum $a = b$.

SATZ 10. *Es sei $g_I V$ nicht die hyperbolische Ebene über $L/I = \boldsymbol{F}_3$. Dann ist* Zentrum $\boldsymbol{O}(V) = \{1, -1\}$.

Bemerkung. Wenn V die hyperbolische Ebene über $L = \boldsymbol{F}_3$ ist, so ist $\boldsymbol{O}(V)$ kommutativ.

Beweis. Jedenfalls gehören 1 und -1 zu Zentrum $\boldsymbol{O}(V)$. Falls andererseits $\sigma \in$ Zentrum $\boldsymbol{O}(V)$, so ist σ mit der Symmetrie τ_A an der nichtisotropen Hyperebene $\langle A \rangle^0$ vertauschbar. σ lässt also die nichtisotrope Gerade $\langle A \rangle$ ungeändert. Die Behauptung folgt aus Satz 9.

2.5. *Symmetrien.* Ein Element $\sigma \in \boldsymbol{O}(V)$ heisst *Involution,* wenn $\sigma^2 = 1$.

SATZ 11. *Sei* $\sigma \in \boldsymbol{O}(V)$ *eine Involution. Setze* $U = \operatorname{Kern}(\sigma + 1)$, $W = \operatorname{Kern}(\sigma - 1)$. *Dann bilden* U *und* W *eine orthogonale Zerlegung von* V, $V = U \perp W$. *Für* σ *haben wir die Darstellung*

$$\sigma = -1 \mid U \perp 1 \mid W, \tag{11}$$

d.h., σ *ist die Symmetrie bezüglich* W. *Ist umgekehrt* $V = U \perp W$ *eine orthogonale Zerlegung von* V, *so ist dazu durch* (11) *eine Involution bestimmt.*

Beweis. 1. Sei σ eine Involution. Sei $U = \operatorname{Kern}(\sigma + 1)$ und $W = \operatorname{Kern}(\sigma - 1)$. Aus $X = (\sigma + 1)X/2 + (\sigma - 1)X/2$ folgt: V wird von U und W erzeugt. Ferner $U \cap W = 0$. Für $X \in U$ und $Y \in W$ haben wir $XY = \sigma X \sigma Y = (-X)Y = -XY = 0$. Es bleibt noch zu zeigen, dass U oder W ein Unterraum ist. Sei A ein nichtisotroper Vektor von V. Dann ist einer der Vektoren $(\sigma + 1)A \in W$ und $(\sigma - 1)A \in U$ nichtisotrop. Wir können also annehmen, dass einer der Räume U und W einen nichtisotropen Vektor B enthält. Wegen $\sigma B = \pm B$ ist $\sigma \mid \langle B \rangle^0$ eine Involution. $\dim \langle B \rangle^0 = \dim V - 1$. Für $\dim V = 1$ ist die Behauptung richtig, wir können also durch Induktion schliessen, dass U oder W ein Unterraum ist.

SATZ 12. *Sei* $\dim V = 2$.

(i) *Jedes Element* $\sigma \in \boldsymbol{O}(V)$ *lässt sich in der Form* τ *oder* $\tau\tau'$ *schreiben, wobei* τ *und* τ' *Symmetrien an nichtisotropen Hyperebenen = Geraden sind. Dann und nur dann, wenn* $\sigma = \tau\tau'$, *gehört* σ *zu* $\boldsymbol{SO}(V)$. *In der Darstellung* $\tau\tau'$ *von* σ *kann* τ *beliebig vorgegeben werden.*

(ii) $\boldsymbol{SO}(V)$ *ist kommutativ.*

(iii) *Falls* $g_I V$ *nicht die hyperbolische Eben über* $L/I = \boldsymbol{F}_3$ *ist, so gibt es in* $\boldsymbol{SO}(V)$ *ein Element* σ *mit* $h_I \sigma^2 \neq 1$.

Beweis. 1. Sei $\sigma \in \boldsymbol{SO}(V)$ und $\tau = \tau_A$ vorgegeben. Wegen $(\sigma^{-1}A - A) \times (\sigma^{-1}A + A) = 0$ ist $\sigma^{-1}A + A$ oder $\sigma^{-1}A - A$ nichtisotrop. In jedem Falle gibt es also einen nichtisotropen Vektor B mit $(\sigma^{-1}A - A)B = 0$ und $(\sigma^{-1}A + A) \in \langle B \rangle$. Es ist daher $\tau_B\sigma^{-1}A = -A$, also $\tau_A\tau_B\sigma^{-1}A = A$. Da $\tau_A\tau_B\sigma^{-1} \in \boldsymbol{SO}(V)$, folgt $\sigma = \tau_A\tau_B$. Da jedes Element von $\boldsymbol{O}(V)$, das nicht zu $\boldsymbol{SO}(V)$ gehört, in der Form $\tau_A\sigma$ mit $\sigma \in \boldsymbol{SO}(V)$ geschrieben werden kann, ist (i) bewiesen.

2. Zum Beweis von (ii) bemerken wir, dass wir, nach (i), zwei Elemente σ_1, σ_2 von $\boldsymbol{SO}(V)$ in der Form $\sigma_1 = \tau\tau_1 = \tau_2\tau_3$, $\sigma_2 = \tau\tau_2$ schreiben können. Damit wird $\sigma_2\sigma_1\sigma_2^{-1} = \tau\tau_2\tau_2\tau_3\tau_2\tau = \tau\tau_3\tau_2\tau = \tau\tau_1\tau\tau = \sigma_1$.

3. Zum Beweis von (iii) nehmen wir an: V ist so beschaffen, dass für jedes $\sigma \in \boldsymbol{SO}(V)$ gilt $h_I\sigma^2 = 1$, d. h., $h_I\boldsymbol{SO}(V) = \boldsymbol{SO}(h_IV)$ besteht nur aus Involutionen. Da $\dim V = 2$, können als Involutionen nur in Frage kommen 1 und -1, das heisst, $\boldsymbol{SO}(g_IV)$ besteht aus 2 Elementen. Da $\boldsymbol{SO}(g_IV)$ den Index 2 in $\boldsymbol{O}(g_IV)$ hat, besteht $\boldsymbol{O}(g_IV)$ aus 4 Elementen, es gibt also nur 2 nichtisotrope Geraden in g_IV, zwei andere Geraden in g_IV müssen isotrop sein, g_IV ist also die hyperbolische Eben über $\boldsymbol{F}_3$.

THEOREM 2. *Sei* $n = \dim V \geqq 2$. *Jedes Element* $\sigma \in \boldsymbol{O}(V)$ *ist das Produkt von* $\leqq 2n - 2$ *Symmetrien an Hyperebenen. Dann und nur dann gehört* σ *zu* $\boldsymbol{SO}(V)$, *wenn die Anzahl der Symmetrien gerade ist.*

FOLGERUNG. *Der Homomorphismus* (2), $h_J\colon \boldsymbol{O}(V) \to \boldsymbol{O}(g_JV)$, *ist surjektiv, und dasselbe gilt für die Einschränkung* $h_J\colon \boldsymbol{SO}(V) \to \boldsymbol{SO}(g_JV)$.

Beweis. 1. Für $n = 2$ folgt die Behauptung aus Satz 12. Wir machen einen Induktionsschluss nach n.

2. Sei $\sigma \in \boldsymbol{O}(V)$. Es gebe einen nichtisotropen Vektor A mit $\sigma A = \epsilon A$, $\epsilon = 1$ oder -1. Dann ist $H = \langle A \rangle^0$ eine nichtisotrope Hyperebene der Dimension $n - 1$ mit $\sigma H = H$. Setze $\tau_A = \tau$. Nach Voraussetzung ist $\sigma \mid H$ das Produkt von $r \leqq 2n - 4$ Symmetrien τ_i, $1 \leqq i \leqq r$. Wir setzen die τ_i durch die Identität auf $\langle A \rangle$ fort und schreiben dafür wieder τ_i. Jenachdem ob $\epsilon = 1$ oder -1 ist, dann $\sigma = \prod \tau_i$ oder $= \tau \prod \tau_i$, $1 \leqq i \leqq r$, d. h., σ ist das Produkt von $\leqq 2n - 3$, Symmetrien an Hyperebenen.

3. Sei A nichtisotrop. Wegen $(\sigma A + A)(\sigma A - A) = 0$ ist $\sigma A + \epsilon A$ für $\epsilon = 1$ oder -1 nichtisotrop. Sei $\tau = \tau_{\sigma A + \epsilon A}$. Dann ist $\tau\sigma A = -\epsilon A$. Nach 2. ist $\tau\sigma$ das Produkt von $\leqq 2n - 3$ Symmetrien, also σ das Produkt von $\leqq 2n - 2$ Symmetrien.

4. Die letzte Behauptung folgt aus der Bemerkung, dass die Symmetrien an Hyperebenen nicht zu $\boldsymbol{SO}(V)$ gehören.

5. Zum Beweis der Folgerung bemerken wir, dass die Abbildung (1), $g_J\colon V(L) \to V(L/J)$, surjektiv ist. Jede Symmetrie an einer nichtisotropen Hyperebene in $\boldsymbol{O}(V(L/J))$ besitzt also ein Urbild in $\boldsymbol{O}(V(L))$.

ERGÄNZUNG ZU THEOREM 2. *Sei J ein Ideal in I. Jedes Element $\sigma \in \boldsymbol{O}(V)$ mit $h_J\sigma = 1$ ist das Produkt von $\leqq (n-1)$ Elementen der Form $(\tau\tau')$, wobei τ, τ' Symmetrien an Hyperebenen sind und $h_J(\tau\tau') = 1$.*

Beweis. Sei A ein nichtisotroper Vektor. Wegen $g_J(\sigma A + A) = 2g_J A$ ist dann auch $(\sigma A + A)$ nichtisotrop. Sei $\tau = \tau_A$ und $\tau' = \tau_{A+\sigma A}$. Dann ist $\tau'\tau\sigma A = A$, also $\sigma = \tau\tau'\sigma'$ mit $\sigma' \mid \langle A \rangle = 1$. Die Behauptung folgt jetzt durch Induktion.

3. Die Kongruenz-Kommutatorgruppen. Theorem 3.

3.1. *Eine Kennzeichnung der Kongruenz-Kommutatorgruppen. Theorem 3.*

THEOREM 3. *Sei* $\dim V \geqq 3$. *J bezeichne ein Ideal von L.*

(i) $\Omega(V, J) =$ *gemischte Kommutatorgruppe von* $\boldsymbol{SO}(V)$ *und* $\boldsymbol{SO}(V, J)$.

(ii) $\Omega(V, J)$ *wird erzeugt von den Elementen*

(12) $(\tau\tau')^2$; τ, τ' *Symmetrien an Hyperebenen mit* $h_J(\tau\tau') = 1$.

FOLGERUNG 1. *Die Kommutatorgruppe $\Omega(V) = \Omega(V, L)$ von $\boldsymbol{O}(V)$ ist zugleich die Kommutatorgruppe von $\boldsymbol{SO}(V) = \boldsymbol{SO}(V, L)$. $\Omega(V)$ enthält das Quadrat eines jeden Elementes aus $\boldsymbol{SO}(V)$. $\boldsymbol{SO}(V)/\Omega(V)$ ist kommutativ und jedes Element hat eine Ordnung $\leqq 2$.*

FOLGERUNG 2. *$\Omega(V, J)$ hat die Ordnung J, d.h., J ist das kleinste Ideal K so, dass $\boldsymbol{O}(V, K) \supset \Omega(V, J)$.*

FOLGERUNG 3. *Der Homomorphismus $h_J\colon \Omega(V) \to \Omega(g_J V)$ ist surjektiv.*

Beweis. 1. Sei $\sigma \in \boldsymbol{O}(V, J)$ und A ein nichtisotrope Vektor. Dann ist $\sigma A + \epsilon A$ nichtisotrop für $\epsilon = 1$ oder -1. Damit wird $\sigma A = -\epsilon\tau_{\sigma A+\epsilon A} A$, also $\tau_{\sigma A} = \tau_{(\tau_{\sigma A+\epsilon A} A)}$. Damit erhalten wir

$$\tau_A\sigma\tau_A^{-1}\sigma^{-1} = \tau_A\tau_{\sigma A} = \tau_A\tau_{(\tau_{\sigma A+\epsilon A} A)} = (\tau_A\tau_{\sigma A+\epsilon A})^2;\ h_J(\tau_A\tau_{\sigma A+\epsilon A}) = 1. \tag{13}$$

2. Wir bezeichnen die von den Elementen (12) erzeugte, invariante

Untergruppe mit $G(J)$. Nach Theorem 2 wird $\boldsymbol{O}(V)$ erzeugt von den Symmetrien an Hyperebenen. Die Formel

$$\rho_1\rho_2\sigma\rho_2^{-1}\rho_1^{-1}\sigma^{-1} = \rho_1(\rho_2\sigma\rho_2^{-1}\sigma^{-1})(\sigma\rho_1^{-1}\sigma^{-1}\rho_1)\rho_1^{-1}$$

zeigt, dass die gemische Kommutatorgruppe $\operatorname{Komm}(\boldsymbol{O}(V), \boldsymbol{O}(V,J))$ erzeugt wird von den Elementen (13) mit $\sigma \in \boldsymbol{O}(V,J)$. Damit haben wir

$$G(J) \supset \operatorname{Komm}(\boldsymbol{O}(V), \boldsymbol{O}(V,J)) \supset \operatorname{Komm}(\boldsymbol{SO}(V), \boldsymbol{SO}(V,J))$$

3. Wir müssen jetzt noch zeigen, dass $G(J)$ enthalten ist in

$$\operatorname{Komm}(\boldsymbol{SO}(V), \boldsymbol{SO}(V,J)),$$

d. h., dass ein erzeugendes Element (12) von $G(J)$ enthalten ist in $\operatorname{Komm}(\boldsymbol{SO}(V), \boldsymbol{SO}(V,J))$. Dazu schreiben wir τ und τ' aus (12) in der Form τ_A und τ_B. Wir zeigen in 4., dass wir uns auf folgenden Fall beschränken können: Die nichtisotropen Vektoren A und B gehören einer nichtisotropen Ebene P an.

Dann ist auch P^0 nichtisotrop, $\dim P^0 = n - 2 \geqq 1$, es gibt also in P^0 einen nichtisotropen Vektor C. Der 3-dimensionale Raum $U = P \perp \langle C \rangle$ ist dann ebenfalls nichtisotrop und wir haben

$$\tau_A = \tau_A \mid U \perp 1 \mid U^0, \qquad \tau_B = \tau_B \mid U \perp 1 \mid U^0.$$

Damit können wir $\tau\tau' = \tau_A\tau_B$ auch in der Form schreiben

$$(14) \quad \tau_A\tau_B = \sigma_A\sigma_B \textit{ mit } \sigma_A = (-1 \cdot \tau_A) \mid U \perp 1 \mid U^0; \sigma_B = (-1 \cdot \tau_B) \mid U \perp 1 \mid U^0.$$

σ_A und σ_B sind Symmetrien an den $(n-2)$-dimensionalen Räumen $\langle A \rangle \perp U^0$ bzw. $\langle B \rangle \perp U^0$, insbesondere gehören also σ_A und σ_B zu $\boldsymbol{SO}(V)$. Wegen (14) können wir das Element (12) auch folgendermassen schreiben:

$$(\tau_A\tau_B)^2 = (\sigma_A\sigma_B)^2 = \sigma_A(\sigma_B\sigma_A)\sigma_A^{-1}(\sigma_B\sigma_A)^{-1} \in \operatorname{Komm}(\boldsymbol{SO}(V), \boldsymbol{SO}(V,J)).$$

4. Es seien A und B nichtisotrope Vektoren. Wir müssen noch zeigen, dass $(\tau_A\tau_B)^2$ dargestellt werden kann als Produkt von Elementen aus $\operatorname{Komm}(\boldsymbol{SO}(V), \boldsymbol{SO}(V,J))$ und von Elementen $(\tau_{A'}\tau_{B'})^2$, wo A' und B' einer nichtisotropen Ebene angehören.

Dazu bemerken wir, dass es zu A und B stets eine Menge nichtisotroper Vektoren A_j, $0 \leqq j \leqq r$, gibt mit folgenden Eigenschaften: $A_0 = A$, $A_r = B$, $h_J\tau_{A_{j-1}}\tau_{A_j} = 1$ und A_{j-1}, A_j in einer nichtisotropen Ebene P_{j-1} gelegen, $1 \leqq j \leqq r$. In der Tat, falls $J \subset I$, so wählen wir eine orthogonale Basis E_i, $1 \leqq i \leqq n$, in V mit $E_1 = A$. Sei $B = \sum E_i a_i$. Setze $A_j = E_1 a_1 + \cdots + E_j a_j$, $r = n$, $P_{j-1} = \langle A_{j-1}, E_j \rangle$. Falls dagegen $J = L$, so gibt es einen Vektor C in

V so, dass $g_I C$ nichtisotrop ist und mit $g_I A$ sowie mit $g_I B$ eine nichtisotrope Ebene aufspannt. Setze $A_1 = C$, $r = 2$.

Mit den so eingeführten Vektoren A_j, $0 \leqq j \leqq r$, haben wir: $\tau_A \tau_B = \tau_{A_0} \tau_{A_r} = \prod \tau_{A_{j-1}} \tau_{A_j}$, $1 \leqq j \leqq r$. Die Formel

$$(\tau_{A_0} \tau_{A_1} \sigma)^2 = (\tau_{A_0} \tau_{A_1})^2 [(\tau_{A_1} \tau_{A_0}) \sigma (\tau_{A_1} \tau_{A_0})^{-1} \sigma^{-1}] \sigma^2$$

zeigt, dass $(\tau_A \tau_B)^2 = (\prod \tau_{A_{j-1}} \tau_{A_j})^2$ als Produkt von Elementen aus Komm $(\boldsymbol{SO}(V), \boldsymbol{SO}(V, J))$ und von Elementen $(\tau_{A_{j-1}} \tau_{A_j})^2$ geschrieben werden kann.

5. Zum Beweis der Folgerung 1 bemerken wir: Nach Theorem 2 wird $\boldsymbol{SO}(V)$ erzeugt von Elementen der Form $(\tau\tau')$, nach dem soeben Bewiesenen gehören die Quadrate dieser Erzeugenden zu $\Omega(V)$. Da Komm $\boldsymbol{SO}(V) = \Omega(V)$, ist also $\boldsymbol{SO}(V)/\Omega(V)$ kommutativ und besitzt ein System von Erzeugenden der Ordnung 2, woraus sich die Behauptung ergibt.

6. Die Ordnung $o(\Omega(V, J))$ von $\Omega(V, J)$ wird erzeugt von den Ordnungen $o(\sigma)$ der Elemente $\sigma \in \Omega(V, J)$. Zum Beweis der Folgerung 2 genügt es also zu zeigen, dass es zu jedem $u \in J$ nichtisotrope Vektoren A und B so gibt, dass das Element $(\tau_A \tau_B)^2$ die Ordnung (u) hat, wo (u) das von u erzeugte Ideal bezeichnet. Falls $(u) = L$, so wählen wir für A und B zwei orthogonale, nichtisotrope Vektoren. Falls $(u) \subset I$, so wählen wir zwei nichtisotrope orthogonale Vektoren A und C und setzen $B = A + Cu$. Dann ist $o((\tau_A \tau_B)^2) = (u)$.

7. Die Folgerung 3 ergibt sich, ähnlich wie die Folgerung zu Theorem 2, aus der angegebenen Erzeugung von $\Omega(V)$.

Ergänzung zu Theorem 3. *Sei* $\dim V \geqq 3$. *Sei* J *ein Ideal in* I. *Ein Element* $\sigma \in \boldsymbol{O}(V)$ *mit* $h_J \sigma = 1$ *ist Produkt von Elementen der Form*

(15) $(\rho\rho')$, *wobei* ρ *und* ρ' *Symmetrien an Unterräumen der Dimension* $n - 2$ *sind und* $h_J(\rho\rho') = 1$.

Beweis. Nach der Ergänzung zu Theorem 2 ist σ Produkt von Elementen $(\tau\tau')$, wo $\tau = \tau_A$ und $\tau' = \tau_B$ Symmetrien an Hyperebenen sind und $h_J(\tau_A \tau_B) = 1$. Nach Teil 4 des vorangehenden Beweises können wir annehmen, dass A und B einer nichtisotropen Ebene angehören. Auf Grund von (14) können wir dann für $\tau\tau' = \tau_A \tau_B$ schreiben $\sigma_A \sigma_B$, d. h., mit $\rho = \sigma_A$, $\rho' = \sigma_B$, (15).

3.2. *Das Zentrum von* $\boldsymbol{SO}(V)$ *und* $\Omega(V)$.

Satz 13. *Sei* $\dim V \geqq 3$. *Wenn* $\sigma \in \boldsymbol{O}(V)$ *vertauschbar ist mit dem Quadrat* ρ^2 *eines jeden Elements* $\rho \in \boldsymbol{SO}(V)$, *dann ist* $\sigma = \pm 1$.

Beweis. 1. Wir zeigen, dass, unter den angegebenen Voraussetzungen, σ jede nichtisotrope Gerade in sich überführt. Dann folgt die Behauptung aus Satz 9.

Sei A ein nichtisotroper Vektor. In $\langle A\rangle^0$ wählen wir zwei zueinander orthogonale, nichtisotrope Vektoren B und C. Setze $P = \langle A, B\rangle$ und $Q = \langle A, C\rangle$. Dann ist $\langle A\rangle = P \cap Q$.

2. Wir schliessen zunächst den Fall aus: $L/I = \boldsymbol{F}_3$ und $g_I P$ oder $g_I Q$ hyperbolisch. Dann gibt es nach Satz 12(iii) ein $\rho \in \boldsymbol{SO}(P)$ mit $g_I \rho^2 \neq 1$. Wir setzen ρ durch die Identität auf P^0 fort und bezeichnen dieses Element wiederum mit ρ. Dann ist also $\rho \in \boldsymbol{SO}(V)$ mit $\rho^2 \mid P^0 = 1$ und $g_I(\rho^2 \mid P) \neq 1$. Wegen $\sigma\rho^2\sigma^{-1} = \rho^2$ gilt auch $\rho^2 \mid \sigma P^0 = 1$, also $\sigma P^0 = P^0$ und folglich $\sigma P = P$. Ebenso ergibt sich $\sigma Q = Q$, also $\sigma\langle A\rangle = \sigma P \cap \sigma Q = P \cap Q = \langle A\rangle$.

3. Sei jetzt $L/I = \boldsymbol{F}_3$ und $g_I P$ sowie $g_I Q$ hyperbolisch. Dann ist $g_I\langle B, C\rangle$ nichthyperbolisch. $P' = \langle A, B + C\rangle$, $Q' = \langle A, B - C\rangle$ sind nichtisotrop und $g_I P'$ und $g_I Q'$ sind nichthyperbolisch. Es ist $\langle A\rangle = P' \cap Q'$. Wir können schliessen wie in 2., dass $\sigma\langle A\rangle = \langle A\rangle$.

4. Sei $L/I = \boldsymbol{F}_3$ und genau eine der Ebenen $g_I P$ und $g_I Q$ hyperbolisch. Wir nehmen an, $g_I P$ is hyperbolisch, der andere Fall wird ganz analog behandelt. Dann ist $g_I\langle B, C\rangle$ hyperbolisch.

$$R = \langle B, A + C\rangle \text{ und } S = \langle B, A - C\rangle$$

sind nichtisotrop und $g_I R$ und $g_I S$ sind nichthyperbolisch. Damit folgt wie in 2., wegen $\langle B\rangle = R \cap S$, $\sigma\langle B\rangle = \sigma R \cap \sigma S = R \cap S = \langle B\rangle$. Also auch $\sigma\langle A + C\rangle = \langle A + C\rangle$ und $\sigma\langle A - C\rangle = \langle A - C\rangle$. Folglich $\sigma\langle A\rangle = \langle A\rangle$ oder $= \langle C\rangle$. Wir wollen den Fall $\sigma\langle A\rangle = \langle C\rangle$ ausschliessen.

Setze $U = \langle A, B, C\rangle$. Jedenfalls ist $\sigma U = U$. Wir bezeichnen die Elemente von $g_I U$ und $\boldsymbol{O}(g_I U)$ jetzt mit einem Querstrich. Auf Grund der Folgerung zu Theorem 2 ist das Element $\bar{\sigma} = h_I\sigma$ mit jedem Quadrat $\bar{\rho}^2$ eines $\bar{\rho} \in \boldsymbol{SO}(\bar{U})$ vertauschbar. Wir betrachten nun das $\bar{\rho} \in \boldsymbol{SO}(\bar{U})$, das gegeben ist durch $\bar{\rho}(\bar{A} + \bar{B}) = (\bar{A} + \bar{B})$, $\bar{\rho}\bar{C} = (\bar{A} + \bar{B}) + \bar{C}$. Man erkennt: Die einzigen Vektoren von $\bar{U}$, die invariant bleiben unter $\bar{\rho}^2$, sind die Vektoren von $\langle \bar{A} + \bar{B}\rangle$. Wegen $\bar{\sigma}\bar{\rho}^2\bar{\sigma}^{-1} = \bar{\rho}^2$ bleiben auch die Elemente von $\bar{\sigma}\langle \bar{A} + \bar{B}\rangle$ invariant, also $\bar{\sigma}\langle \bar{A} + \bar{B}\rangle = \langle \bar{A} + \bar{B}\rangle$, also $\bar{\sigma}\langle \bar{A}\rangle = \langle \bar{A}\rangle$, $\sigma\langle A\rangle = \langle A\rangle$.

SATZ 14. *Sei* $\dim V \geqq 3$. *Der Zentralisator von* $\boldsymbol{SO}(V)$ *in* $\boldsymbol{O}(V)$ *ist gleich dem Zentralisator von* $\Omega(V)$ *in* $\boldsymbol{O}(V)$ *und besteht aus* $\{1, -1\}$. *Daher ist* $\text{Zentrum}\,\boldsymbol{SO}(V) = \boldsymbol{SO}(V) \cap \text{Zentrum}\,\boldsymbol{O}(V)$ *und* $\text{Zentrum}\,\Omega(V) = \Omega(V) \cap \text{Zentrum}\,\boldsymbol{O}(V)$.

Beweis. Nach Satz 13 ist der Zentralisator der Menge von Quadraten ρ^2 von Elementen $\rho \in \boldsymbol{SO}(V)$ gleich $\{1, -1\}$. Nach Folgerung 1 zu Theorem 3 gehören diese ρ^2 zu $\Omega(V)$. Nach Satz 10 ist Zentrum $\boldsymbol{O}(V) = \{1, -1\}$.

SATZ 15. *Sei* $\dim V \geqq 3$, *sei* J *ein Ideal in* I. *Dann ist* $\boldsymbol{SO}(V,J)$ $=$ *Gruppe der* $\sigma \in \boldsymbol{SO}(V)$ *mit* $h_J\sigma \in \{1, -1\}$, *für* $\dim V$ *gerade, oder, mit* $h_J\sigma = 1$, *für* $\dim V$ *ungerade.*

Beweis. $\boldsymbol{SO}(V,J) =$ Gruppe der $\sigma \in \boldsymbol{SO}(V)$ mit

$$h_J\sigma \in h_J\boldsymbol{SO}(V) = \boldsymbol{SO}(g_JV)$$

und $h_J\sigma \in$ Zentrum $\boldsymbol{O}(g_JV)$, d.h., $h_J\sigma \in \boldsymbol{SO}(g_JV) \cap$ Zentrum $\boldsymbol{O}(g_JV) =$ Zentrum $\boldsymbol{SO}(g_JV)$.

4. Anwendungen der Cliffordalgebra. Theorem 4 und 5.

4.1. *Die Cliffordalgebra über* V. Für die weiteren Untersuchungen benötigen wir die wichtigsten Eigenschaften der Cliffordalgebra über V. Bei der Herleitung dieser Eigenschaften begnügen wir uns mit Andeutungen der Beweise, sobald diese ebenso verlaufen wie in dem Fall, dass L ein Körper ist. Wir verweisen, neben Dieudonné [4] und Artin [1], auf Bourbaki [2], wo auch die Cliffordalgebra über einem freien Modul betrachtet wird.

Sei $T(V)$ die Tensoralgebra über V. Mit S bezeichnen wir die Unteralgebra von $T(V)$, die erzeugt wird von den Elementen

$$X \otimes X - X^2, \quad X \in V \tag{16}$$

von $T(V)$, wobei wir V als Untermodul von $T(V)$ auffassen.

Unter der *Cliffordalgebra über* V, $C(V)$, verstehen wir die Quotientenalgebra $T(V)/S$. Das Bild eines $X \in V \subset T(V)$ in $C(V)$ bezeichnen wir wieder mit X. Die Multiplikation in $C(V)$ bezeichnen wir mit $(\alpha, \beta) \rightarrow \alpha \circ \beta$.

Aus (16) haben wir die Relation

$$X \circ Y + Y \circ X = 2XY. \tag{17}$$

Da V eine Basis besitzt, hat auch $C(V)$ eine Basis. Und zwar ist, wenn E_i, $1 \leqq i \leqq n = \dim V$, eine orthogonale Basis von V ist, $E_{i_1} \circ \cdots \circ E_{i_k}$, $i_1 < \cdots < i_k$, $(k = 0, \cdots, n)$ eine Basis von $C(V)$. Also $\dim C(V) = 2^n$. Aus (17) folgt: $E_i \circ E_k + E_k \circ E_i = 0$ für $i \neq k$, und $E_i \circ E_i = E_i^2$.

Mit $C^+(V)$ bezeichnen wir die Unteralgebra von $C(V)$, die erzeugt wird von den Produkten einer geraden Anzahl von Vektoren aus V.

Das Zentrum von $C(V)$ ist gleich L, falls $n = \dim V$ gerade, und gleich

$L + e_V L$, falls n ungerade, wobei e_V das Produkt aus den n Elementen einer orthogonalen Basis von V ist. Es folgt $C^+(V) \cap \text{Zentrum}\ C(V) = L$.

Die Elemente $\alpha \in C(V)$, die mit jedem $X \in V$ antikommutativ sind, d. h. $\alpha \circ X = -X \circ \alpha$, sind von der Form $\alpha = 0$ oder falls $\dim V$ gerade, $\alpha = e_V c$, $c \in L$. In jedem Falle gehören diese Elemente also zu $C^+(V)$.

Sei $\alpha \in C(V)$ invertierbar. $s(\alpha)$ bezeichne den inneren Automorphismus: $\beta \in C(V) \rightarrow s(\alpha)\beta = \alpha \circ \beta \circ \alpha^{-1} \in C(V)$. Unter der *Cliffordgruppe von* V, $R(V)$, verstehen wir die multiplikative Gruppe derjenigen invertierbaren Elemente $\alpha \in C(V)$, für die $s(\alpha)V = V$ ist. $R(V) \cap C^+(V)$ heisst *spezielle Cliffordgruppe von* V, $D(V)$.

Wir behaupten, dass, für $\alpha \in R(V)$, $s(\alpha) | V \colon V \rightarrow V$ eine Isometrie von V ist. In der Tat, $s(\alpha)$, angewandt auf (17), lässt die rechte Seite von (17) ungändert, während die linke übergeht in $s(\alpha)X \circ s(\alpha)Y + s(\alpha)Y \circ s(\alpha)X = 2s(\alpha)Xs(\alpha)Y$. Den durch $\alpha \in R(V) \rightarrow s(\alpha) | V \in \boldsymbol{O}(V)$ erklärten Homomorphismus bezeichnen wir mit s. Wegen $D(V) \cap \text{Zentrum}\ C(V) = L^*$ ist $\text{Kern}(s \,|\, D(V)) = L^*$.

Zu der Cliffordgruppe von V, $R(V)$, gehören insbesondere die nichtisotropen Vektoren B von V. Denn durch B/B^2 ist B^{-1} erklärt und für $X \in V$ haben wir

$$\begin{aligned} (18) \qquad s(B)X = B \circ X \circ B^{-1} &= (-X \circ B + 2BX) \circ B^{-1} \\ &= -X + B(2BX/B^2) = -1\tau_B X \in V. \end{aligned}$$

Hier bezeichnet τ_B die Symmetrie an $\langle B \rangle^0$.

Da nach Theorem 2 jedes $\sigma \in \boldsymbol{O}(V)$ eine Darstellung als Produkt von Symmetrien τ_{B_i} besitzt, wo die B_i nichtisotrope Vektoren sind, folgt aus (18)

$$\begin{aligned} &\sigma = \tau_{B_1} \cdots \tau_{B_r} \in \boldsymbol{O}(V) \text{ impliziert, mit } X \in V, \\ (19) \qquad &\sigma X = (-1)^r s(B_1 \circ \cdots \circ B_r) X \\ &\qquad = (-1)^r B_1 \circ \cdots \circ B_r \circ X \circ B_r^{-1} \circ \cdots \circ B_1^{-1}. \end{aligned}$$

Sei $\alpha \in D(V)$. $s(\alpha) | V = \sigma$ habe die in (19) angegebene Darstellung. Aus (19) folgt $s(\alpha) = (-1)^r s(B_1 \circ \cdots \circ B_r)$, also $s(\alpha^{-1} \circ B_1 \circ \cdots \circ B_r) = (-1)^r$. r muss gerade sein. Denn wäre r ungerade, so würde, da $\alpha \in C^+(V)$, $\beta = \alpha^{-1} \circ B_1 \circ \cdots \circ B_r$ nicht zu $C^+(V)$ gehören und mit jedem $X \in V$ antikommutativ sein, was wir oben ausgeschlossen haben. Also ist r gerade, $\sigma \in \boldsymbol{SO}(V)$, $\beta \in D(V)$. Wegen $\text{Kern}(s \,|\, D(V)) = L^*$ haben wir $\alpha = cB_1 \circ \cdots \circ B_r$, mit $c \in L^*$ oder, mit $B'_1 = B_1 c$, $\alpha = B'_1 \circ \cdots \circ B_r$. Zusammenfassend gilt also

Jedes Element α *der speziellen Cliffordgruppe* $D(V)$ *von* V *ist das*

Produkt einer geraden Anzahl von nichtisotropen Vektoren. Durch $\alpha \in D(V) \to s(\alpha) \mid V \in \boldsymbol{O}(V)$ *ist ein surjektiver Homomorphismus*

$$s: D(V) \to \boldsymbol{SO}(V) \tag{20}$$

gegeben mit

$$\mathrm{Kern}(s \mid D(V)) = L^*;\ D(V)/L^* \textit{ isomorph } \boldsymbol{SO}(V). \tag{21}$$

Es bezeichne $\alpha \to \bar{\alpha}$ den natürlichen Antiautomorphismus von $C(V)$, der in der Umkehrung der Reihenfolge der Multiplikation besteht. Für $\alpha = B_1 \circ \cdots \circ B_r \in D(V)$ haben wir dann $\alpha \circ \bar{\alpha} = B_1 \circ \cdots \circ B_r \circ B_r \circ \cdots \circ B_1 = B_1^2 \cdots B_r^2 \in L^*$.

$$N: \alpha \in D(V) \to N(\alpha) = \alpha \circ \bar{\alpha} \in L^* \tag{22}$$

ist ein Homomorphismus, den wir *(Clifford-)Norm* nennen. Kern N heisst *reduzierte Cliffordgruppe von* V, $D_0(V)$. Das Bild $sD_0(V)$ von $D_0(V)$ *in* $\boldsymbol{SO}(V)$ heisst *reduzierte orthogonale Gruppe von* V, $\boldsymbol{O}'(V)$. Da Kern $(s \mid D_0(V)) = \{1, -1\}$, folgt

$$D_0(V)/\{1, -1\} \textit{ isomorph } \boldsymbol{O}'(V). \tag{23}$$

Sei $\sigma \in \boldsymbol{SO}(V)$. Nach (21) unterscheiden sich zwei Elemente α und α' von $D(V)$ mit $s(\alpha) = s(\alpha') = \sigma$ um ein Element aus L^*. Zu $\sigma \in \boldsymbol{SO}(V)$ ist daher $N(\alpha)L^{*2}$ mit $s(\alpha) = \sigma$ eindeutig festgelegt. Der so erklärte Homomorphismus

$$\theta: \boldsymbol{SO}(V) \to L^*/L^{*2} \tag{24}$$

heisst *Spinornorm*.

Mit Hilfe von (19) erkennen wir: Falls $\sigma \in \boldsymbol{SO}(V)$ in der Form (19) geschrieben ist, so ist $\theta(\sigma) = B_1^2 \cdots B_r^2 L^{*2}$. Insbesondere, wenn E_i, $1 \leqq i \leqq n = \dim V$, eine orthogonale Basis von V ist, und $-1 \in \boldsymbol{SO}(V)$, so wird $\theta(-1) = E_1^2 \cdots E_n^2 L^{*2}$.

Kern $\theta = \boldsymbol{O}'(V)$.

4. 2. *Eine weitere Kennzeichnung der Kongruenz-Kommutatorgruppen. für* ind $V \geqq 1$. *Theorem* 4.

SATZ 16. *Sei* $\dim V = 2$. $\theta(-1) = -1 \cdot L^{*2}$ *ist äquivalent mit* ind $V = 1$.

Beweis. Falls ind $V = 1$, so sei N, M ein hyperbolisches Paar in V. $E_1 = N + M/2$, $E_2 = N - M/2$ ist eine orthogonale Basis von V. $\theta(-1)$

$= E_1^2 E_2^2 L^{*2} = -1 \cdot L^{*2}$. Wenn umgekehrt, für eine orthogonale Basis E_1, E_2 von V, $E_1^2 E_2^2 = -c^2$, so ist $E_1 E_2^2 + E_2 c$ ein isotroper Vektor in V.

THEOREM 4. (1. Teil) *Sei* $\dim V = 2$. *Sei* J *ein Ideal von* L *mit* $J \subset I$. *Sei*

$$(25) \qquad \theta_J = \theta \times h_J \colon \sigma \in \boldsymbol{SO}(V) \rightarrow (\theta(\sigma), h_J\sigma) \in L^*/L^{*2} \times \boldsymbol{SO}(g_J V).$$

(i) $\operatorname{Kern} \theta = \Omega(V)$. $\operatorname{Kern} \theta_J = \Omega(V, J)$.

(ii) *Sei* $\operatorname{ind} V = 1$. $\boldsymbol{SO}(V)/\Omega(V)$ *ist isomorph* $\operatorname{Bild}(\theta \mid \boldsymbol{SO}(V)) = L^*/L^{*2}$. $\boldsymbol{SO}(V, J)/\Omega(V, J)$ *ist isomorph* $\operatorname{Bild}(\theta_J \mid \boldsymbol{SO}(V, J))$. *Falls* $L/I \neq \boldsymbol{F}_3$, *ist* $\boldsymbol{SO}(V, J)/\Omega(V, J)$ *isomorph*

$$\operatorname{Bild}(\theta \mid \boldsymbol{SO}(V, J)) = g_J^{-1}\{1, -1\}/L^{*2}.$$

Beweis. 1. Beweis von (i). Zunächst ist klar: $\Omega(V) \subset \operatorname{Kern} \theta$ und $\Omega(V, J) \subset \operatorname{Kern} \theta_J$. Sei umgekehrt $\sigma \in \operatorname{Kern} \theta$. Nach Satz 12 lässt σ sich in der Form $\tau_A \tau_B$ schreiben, mit vorgegebenem nichtisotropen A. Es ist also $A^2 B^2 \in L^{*2}$. Daher gibt es $b \in L^*$ so, dass $C = Bb$ und $C^2 = A^2$. Nach der Ergänzung zu Theorem 1 gibt es $\rho \in \boldsymbol{SO}(V)$ mit $\rho A = C$. Damit wird $\sigma = \tau_A \tau_B = \tau_A \tau_C = \tau_A \tau_{\rho A} = \tau_A \rho \tau_A \rho^{-1} \in \Omega(V, L) = \Omega(V)$. Sei jetzt noch $h_J\sigma = 1$ also $\sigma \in \operatorname{Kern} \theta_J$. $h_J\sigma = h_J \tau_A \tau_{\rho A} = 1$ bedeutet: $h_J\rho \langle g_J A \rangle = \langle g_J A \rangle$, d. h., $h_J\rho$ lässt die nichtisotrope Gerade $\langle g_J A \rangle$ fest, oder auch, $h_J\rho$ ist vertauschbar mit der Symmetrie $\tau_{g_J A}$. Da A beliebig war, ist $h_J\rho \in \operatorname{Zentrum} \boldsymbol{O}(g_J V)$, also $\rho \in \boldsymbol{SO}(V, J)$, also $\sigma = \tau_A \rho \tau_A \rho^{-1} \in \Omega(V, J)$.

2. Beweis von (ii). Nach (i) ist jedenfalls $\boldsymbol{SO}(V)/\Omega(V)$ isomorph $\operatorname{Bild}(\theta \mid \boldsymbol{SO}(V))$, und dies ist enthalten in L^*/L^{*2}. Ist andererseits $aL^{*2} \in L^*/L^{*2}$ vorgegeben, so ist $\sigma = \tau_{N+M} \tau_{N+Ma} \in \boldsymbol{SO}(V)$ und $\theta(\sigma) = aL^{*2}$, also $\operatorname{Bild} \theta = L^*/L^{*2}$. Damit ist der erste Teil von (ii) bewiesen. Sei jetzt $J \subset I$. Nach (i) ist jedenfalls $\boldsymbol{SO}(V, J)/\Omega(V, J)$ isomorph $\operatorname{Bild}(\theta_J \mid \boldsymbol{SO}(V, J)) =$ Gruppe der Paare $(\theta(\sigma), h_J\sigma)$ mit $\sigma \in \boldsymbol{SO}(V, J)$. Wir setzen jetzt $L/I \neq \boldsymbol{F}_3$ voraus. Nach Satz 10 ist in diesen Paaren dann stets $h_J\sigma = 1$ oder -1, also $g_J\theta(\sigma) = \theta(h_J\sigma) = \theta(1) = (L/J)^{*2}$ oder $= \theta(-1) = -1 \cdot (L/J)^{*2}$, nach Satz 16. Also $\operatorname{Bild}(\theta \mid \boldsymbol{SO}(V, J)) \subset g_J^{-1}\{1, -1\}/L^{*2}$. Ist $aL^{*2} \in g_J^{-1}\{1, -1\}/L^{*2}$ gegeben, wobei wir annehmen können, dass $g_J a \in \{1, -1\}$, so ist $\sigma = \tau_{N+M} \tau_{N+Ma} \in \boldsymbol{SO}(V, J)$ mit $\theta(\sigma) = aL^{*2}$. Also $\operatorname{Bild}(\theta \mid \boldsymbol{SO}(V, J)) = g_J^{-1}\{1, -1\}/L^{*2}$. Es bleibt noch zu zeigen, dass $\operatorname{Kern}(\theta \mid \boldsymbol{SO}(V, J)) = \Omega(V, J)$ ist. Für ein $\sigma \in \boldsymbol{SO}(V, J)$ mit $\theta(\sigma) = L^{*2}$ ist $g_J\theta(\sigma) = \theta(h_J\sigma) = (L/J)^{*2}$, also $h_J\sigma = 1$, also $\sigma \in \Omega(V, J)$.

THEOREM 4. (2. Teil) *Sei* $\dim V \geqq 3$, $\operatorname{ind} V \geqq 1$. *Sei* J *ein Ideal in* I. θ_J *sei erklärt durch* (25).

(i) $\operatorname{Kern} \theta = \Omega(V)$. $\operatorname{Kern} \theta_J = \Omega(V, J)$.

(ii) $\boldsymbol{SO}(V)/\Omega(V)$ *ist isomorph* $\operatorname{Bild}(\theta \mid \boldsymbol{SO}(V)) = L^*/L^{*2}$.
$\boldsymbol{SO}(V,J)/\Omega(V,J)$ *ist isomorph* $\operatorname{Bild}(\theta_J \mid \boldsymbol{SO}(V,J)) =$ *Untergruppe der Paare* $(aL^{*2}, \bar{\sigma}) \in g_J^{-1} \operatorname{Bild}(\theta \mid \operatorname{Zentrum} \boldsymbol{SO}(g_J V))/L^{*2} \times \operatorname{Zentrum} \boldsymbol{SO}(g_J V)$ *mit* $g_J a L^{*2} = \theta(\bar{\sigma})$.

(iii) $(\boldsymbol{SO}(V,J) \cap \Omega(V))/\Omega(V,J)$ *ist isomorph* $\operatorname{Zentrum} \Omega(g_J V)$.

FOLGERUNG. (i) $\operatorname{Kern}(h_J \colon \Omega(V) \to \Omega(g_J V)) = \Omega(V, J)$.

(ii) *Falls* $\dim V$ *ungerade, also* $\operatorname{Zentrum} \boldsymbol{SO}(g_J V) = 1$, *so ist* $\boldsymbol{SO}(V,J)/\Omega(V,J)$ *isomorph* $g_J^{-1}(L/J)^{*2}/L^{*2}$.

(iii) *Falls* $\dim V$ *ungerade, so ist* $\operatorname{Zentrum} \Omega(g_J V) = 1$ *und folglich* $\boldsymbol{SO}(V,J) \cap \Omega(V) = \Omega(V,J)$.

Beweis. 1. Beweis von (i). Offenbar $\Omega(V) \subset \operatorname{Kern} \theta$ und $\Omega(V,J) \subset \operatorname{Kern} \theta_J$. Sei jetzt $\sigma \in \operatorname{Kern} \theta$. Nach Theorem 2 lässt $\sigma \in \boldsymbol{SO}(V)$ sich als Produkt $\prod \tau_A \tau_{A'}$ von Elementen $\tau_A \tau_{A'}$ schreiben, wo τ_A und $\tau_{A'}$ Symmetrien an Hyperebenen sind. Wegen $\operatorname{ind} V \geqq 1$ gibt es in V ein hyperbolisches Paar N, M. Setze $\langle N, M \rangle = P$. Zu jedem Paar A, A' erklären wir B und B' in P durch $B = N + MA^2/2$, $B' = N + MA'^2/2$. Wir haben $B^2 = A^2$ und $B'^2 = A'^2$. Daher gibt es ϵ und ϵ' mit den Werten 1 oder -1 so, dass $C = A + \epsilon B$ und $C' = A' + \epsilon' B'$ beide nichtisotrop sind. Es ist $\tau_C B = -\epsilon A$ und $\tau_C B' = -\epsilon' A'$. Daher

$$\tau_A \tau_{A'} = \tau_C \tau_B \tau_C \tau_{C'} \tau_{B'} \tau_{C'} = [\tau_{C'}[(\tau_{C'} \tau_C) \tau_B (\tau_{C'} \tau_C)^{-1} \tau_B^{-1}] \tau_{C'}^{-1}] [\tau_{C'} (\tau_B \tau_{B'}) \tau_{C'}^{-1} (\tau_B \tau_{B'})^{-1}] \tau$$

d. h., $\tau_A \tau_{A'} = \omega_{AA'} \tau_B \tau_{B'}$ mit $\omega_{AA'} \in \Omega(V)$. Also auch $\sigma = \prod \tau_A \tau_{A'} = \omega \prod \tau_B \tau_{B'}$ mit $\omega \in \Omega(V)$. Setze $\prod \tau_B \tau_{B'} = \rho$. Wegen $\rho \mid P^0 = 1$ können wir ρ auffassen als Element von $\boldsymbol{SO}(P)$, und wegen $\theta(\sigma) = L^{*2}$ und $\theta(\omega) = L^{*2}$ ist auch $\theta(\rho) = L^{*2}$, also nach Theorem 4, Teil 1, (i), $\rho \in \Omega(P)$, oder auch $\rho \in \Omega(V)$, also auch $\sigma = \omega\rho \in \Omega(V)$.

Sei jetzt ausserdem noch $h_J \sigma = 1$, $J \subset I$, d. h., $\sigma \in \operatorname{Kern} \theta_J$. Nach der Ergänzung zu Theorem 2 können wir σ als Produkt $\prod \tau_A \tau_{A'}$ mit $h_J \tau_A \tau_{A'} = 1$ schreiben, d. h., $\langle g_J A \rangle = \langle g_J A' \rangle$. Wir können daher annehmen: $g_J A = g_J A'$. Dann ist auch, für die oben konstruierten Vektoren, $g_J B = g_J B'$ und, mit $\epsilon = \epsilon'$, $g_J C = g_J C'$. Daher auch in $\tau_A \tau_{A'} = \omega_{AA'} \tau_B \tau_{B'}$: $\omega_{AA'} \in \Omega(V,J)$, also in $\sigma = \omega\rho$: $\omega \in \Omega(V,J)$, und wegen $h_J \sigma = h_J \omega = 1$: $h_J \rho = 1$, d. h., nach Theorem 4, Teil 1, (i), $\rho \in \Omega(V,J)$, also auch $\sigma = \omega\rho \in \Omega(V,J)$.

2. Beweis von (ii). Nach (i) ist jedenfalls $\boldsymbol{SO}(V)/\Omega(V)$ isomorph Bild$(\theta \mid \boldsymbol{SO}(V))$, und dies ist enthalten in L^*/L^{*2}. Sei N, M ein hyperbolisches Paar in V, setze $\langle N, M\rangle = P$. Nach Theorem 4, 1. Teil, (ii), gibt es $\sigma \in \boldsymbol{SO}(P)$ so, dass $\theta(\sigma)$ einen vorgegebenen Wert in L^*/L^{*2} annimmt. Indem wir σ als Element von $\boldsymbol{SO}(V)$ auffassen, erhalten wir Bild$(\theta \mid \boldsymbol{SO}(V)) = L^*/L^{*2}$. Damit ist der erste Teil in (ii) bewiesen.

Sei jetzt $J \subset I$. Nach (i) ist jedenfalls $\boldsymbol{SO}(V,J)/\Omega(V,J)$ isomorph Bild$(\theta_J \mid \boldsymbol{SO}(V,J)) =$ Gruppe der Paare $(\theta(\sigma), h_J\sigma)$ mit $\sigma \in \boldsymbol{SO}(V,J)$, also, nach Satz 15, mit $h_J\sigma = 1$ oder, falls $\dim V$ gerade, -1. Sei $(aL^{*2}, \bar{\sigma})$ gegeben mit $g_J aL^{*2} = \theta(\bar{\sigma}) = \theta(1) = (L/J)^{*2}$. Wir können annehmen: $g_J a = 1$. Für $\sigma = \tau_{N+M}\tau_{N+Ma} \in \boldsymbol{SO}(V,J)$ haben wir dann $(\theta(\sigma), h_J\sigma) = (aL^{*2}, 1)$.

Für $\dim V$ gerade müssen wir noch den Fall betrachten: aL^{*2} gegeben mit $g_J aL^{*2} = \theta(-1 \mid g_J V)$. Dazu wählen wir in P^0 eine orthogonale Basis E_j, $3 \leqq j \leqq n = \dim V$. Zusammen mit $N+M$, $N-M$ liefert dies eine orthogonale Basis von V. Wir setzen

$$(N+M)^2(N-M)^2E_3{}^2\cdots E_n{}^2 = -4E_3{}^2\cdots E_n{}^2 = \Delta.$$

Dann ist $\theta(-1) = \Delta L^{*2}$. Sei also $g_J aL^{*2} = g_J\Delta L^{*2}$. Wir können annehmen: $g_J a = g_J\Delta$. Dann haben wir für

$$\sigma = \tau_{N+M}\tau_{N-Ma/\Delta}\tau_{E_3}\cdots\tau_{E_n} \in \boldsymbol{SO}(V,J) : (\theta(\sigma), h_J\sigma) = (aL^{*2}, -1).$$

3. Beweis von (iii). Nach (ii) ist $(\boldsymbol{SO}(V,J) \cap \Omega(V))/\Omega(V,J)$ isomorph zu Bild$(\theta_J \mid \boldsymbol{SO}(V,J) \cap \Omega(V)) =$ Gruppe der Paare $(\theta(\sigma), h_J\sigma)$ mit $\theta(\sigma) = L^{*2}$ und $h_J\sigma \in$ Zentrum $\boldsymbol{SO}(g_J V)$. Das heisst, $\theta(h_J\sigma) = g_J\theta(\sigma) = (L/J)^{*2}$, also nach (i), $h_J\sigma \in \Omega(g_J V)$. Das Bild ist also isomorph zur Gruppe Zentrum $\boldsymbol{SO}(g_J V) \cap \Omega(g_J V) =$ Zentrum $\Omega(g_J V)$, nach Satz 14.

4.3. *Über die Gruppen* $\boldsymbol{SO}(V)$ *für* $\dim V \leqq 4$. *Theorem* 5.

SATZ 17. *Falls* $\dim V \leqq 4$, *so besteht die spezielle Cliffordgruppe* $D(V)$ *von* V *aus den Elementen* α *von* $C^+(V)$, *für die* $\alpha \circ \bar{\alpha} \in L^*$.

Beweis. Nach (22) ist für jedes $\alpha \in D(V)$ $\alpha \circ \bar{\alpha} \in L^*$. Wenn umgekehrt für $\alpha \in C^+(V)$ gilt $\alpha \circ \bar{\alpha} \in L^*$, so ist durch $\bar{\alpha}(1/\alpha \circ \bar{\alpha})$ ein Inverses α^{-1} von α erklärt. Für $X \in V \subset C(V)$ haben wir $s(\alpha)X = \alpha \circ X \circ \alpha^{-1} = \alpha \circ X \circ \bar{\alpha}/\alpha \circ \bar{\alpha}$. Wir erkennen, dass $s(\alpha)X$ invariant ist unter dem kanonischen Antiautomorphismus von $C(V)$. Da $s(\alpha)X$ nicht zu $C^+(V)$ gehört und $\dim V \leqq 4$, muss daher $s(\alpha)X$ zu V gehören, also $\alpha \in D(V)$.

THEOREM 5. (i) *Sei* $\dim V = 2$.

(a) *Sei* $\operatorname{ind} V = \operatorname{ind} g_I V = 0$. *Dann ist* $C^+(V)$ *ein lokaler Ring* $L' = L((-\Delta)^{\frac{1}{2}})$, *der aus* L *durch quadratische Erweiterung mit einem Element* $-\Delta, \Delta \in \theta(-1)$, *entsteht.* $\boldsymbol{SO}(V)$ *ist isomorph* L'^*/L^*.

(b) *Sei* $\operatorname{ind} V = 1$. *Dann ist* $\boldsymbol{SO}(V)$ *isomorph* L^*.

Beweis. 1. Sei $\operatorname{ind} V = \operatorname{ind} g_I V = 0$. Sei E_1, E_2 eine orthogonale Basis von V. Setze $E_1 \circ E_2 = e_V$ und $e_V \circ e_V = -E_1^2 E_2^2 = \Delta$. Nach Satz 16 ist $g_I(-\Delta)$ nicht Quadrat in L/I. $C^+(V) = L + e_V L$ ist also ein lokaler Ring L' mit grösstem Ideal $I' = I + e_V I$. Für $\alpha = a + e_V b$ wird $\alpha \circ \bar{\alpha} = a^2 + \Delta b^2$. $\alpha \circ \bar{\alpha} \in L^*$ also genau dann, wenn $\alpha \in L'^*$. Nach Satz 17 ist also $D(V) = L'^*$, nach (21) ist $\boldsymbol{SO}(V)$ isomorph L'/L^*.

2. Sei $\operatorname{ind} V = 1$. Sei N, M ein hyperbolisches Paar in V. Setze $E_1 = N + M/2$, $E_2 = N - M/2$. Für $e_V = E_1 \circ E_2$ haben wir $e_V \circ e_V = 1$. Setze $f = (1 + e_V)/2$, $f' = (1 - e_V)/2$. Damit wird $C^+(V) = L + e_V L = fL + f'L$ isomorph zu $L \times L$, also, nach Satz 17, $D(V)$ isomorph zu $L^* \times L^*$ und $\boldsymbol{SO}(V)$ isomorph L^*.

THEOREM 5. (ii) *Sei* $\dim V = 3, \operatorname{ind} V = 1$. *Dann ist* $\boldsymbol{SO}(V)$ *isomorph zu* $PGL(2, L)$. *Dabei geht* $\Omega(V)$ *über in* $PSL(2, L)$.

Beweis. Sei N, M ein hyperbolisches Paar in V. Wir betrachten eine orthogonale Basis von V der Form $E_1 = N + M/2, E_2 = N - M/2, E_3$. Setze $E_3^2 = a \in L^*$. Die Cliffordalgebra $C^+(V)$ besitzt als Basis die Elemente 1, $i_1 = E_2 \circ E_3$, $i_2 = E_3 \circ E_1$, $i_3 = E_1 \circ E_2$. Damit haben wir

$$i_1 \circ i_1 = a,\ i_1 \circ i_2 = -i_2 \circ i_1 = -i_3 a,\ i_3 \circ i_1 = -i_1 \circ i_3 = i_2,$$
$$i_2 \circ i_3 = -i_3 \circ i_2 = -i_1,\ i_2 \circ i_2 = -a,\ i_3 \circ i_3 = 1.$$

Wenn wir also der Basis $\{1, i_1, i_2, i_3\}$ von $C^+(V)$ die Basis

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

der L-Algebra $M(2, L)$ der $(2,2)$-Matrizen über L zuordnen, erhalten wir einen Isomorphismus

$$\phi : C^+(V) \to M(2, L) \quad \textit{mit} \quad \alpha \circ \bar{\alpha} = \det \phi(\alpha). \tag{26}$$

Wegen Satz 17 liefert ϕ, (26), einen Isomorphismus von $D(V)$ auf $GL(2, L)$ = multiplikative Gruppe der invertierbaren Matrizen in $M(2, L)$. Das Zentrum L^* von $D(V)$ geht unter ϕ über in das Zentrum von $GL(2, L)$. Wegen (21) ist also $\boldsymbol{SO}(V)$ isomorph zu $D(V)/L^*$ und dies ist isomorph zu

$$PGL(2, L) = GL(2, L)/\text{Zentrum}\, GL(2, L).$$

Aus (26) erkennen wir, dass $D_0(V)$ unter ϕ übergeht in $SL(2,L)$. Wegen Theorem 4 (i) und (23) ist $\Omega(V) = \boldsymbol{O}'(V)$ isomorph $D_0(V)/(D_0(V) \cap L^*)$ und dies ist also isomorph zu $PSL(2,L) = SL(2,L)/(SL(2,L) \cap \text{Zentrum } GL(2,L)) = SL(2,L)/\{1,-1\}$.

ERGÄNZUNG ZU THEOREM 5 (ii). *Sei J ein Ideal in I. Bei dem Isomorphismus von $\boldsymbol{SO}(V)$ auf $PGL(2,L)$ geht $\boldsymbol{SO}(V,J)$ über in $PGC(2,L,J)$ und $\Omega(V,J)$ geht über in $PSC(2,L,J)$.*

Bemerkung. Für die Definition und die wichtigsten Eigenschaften der Gruppen $GC(2,L,J)$ und $SC(2,L,J)$ vgl. den Anhang.

Beweis. Bei dem Isomorphismus ϕ, (26), besteht $\phi^{-1}GC(2,L,J)$ aus den $\alpha \in D(V)$ mit $h_J\alpha \in \text{Zentrum } D(g_JV) = (L/J)^*$, wobei wir mit $h_J\colon D(V) \to D(g_JV)$ wiederum den natürlichen Homomorphismus bezeichnen. Bei dem Homomorphismus s, (20), geht $h_J^{-1}(L/J)^* = \phi^{-1}GC(2,L,J) \subset D(V)$ über in die Gruppe der Elemente $\sigma \in \boldsymbol{SO}(V)$ mit $h_J\sigma = 1$, d. h., da Zentrum $\boldsymbol{SO}(g_JV) = 1$, in die Gruppe $\boldsymbol{SO}(V,J)$.

$\phi^{-1}SC(2,L,J) \subset D(V)$ ist gleich $h_J^{-1}(L/J)^* \cap D_0(V)$. Bei s, (20), geht diese Gruppe über in $\boldsymbol{SO}(V,J) \cap \Omega(V) = \Omega(V,J)$, nach der Folgerung (iii) zu Theorem 4.

THEOREM 5. (iii) *Sei* $\dim V = 4$.

(a) *Sei* $\operatorname{ind} V = \operatorname{ind} g_IV = 1$. *Dann ist* Zentrum $C^+(V) = L + e_VL$ *ein lokaler Ring $L' = L(\Delta^{\frac{1}{2}})$, der aus L durch quadratische Erweiterung mit einem Element $\Delta \in \theta(-1)$ entsteht. $P\boldsymbol{SO}(V) = \boldsymbol{SO}(V)/\{1,-1\}$ ist isomorph zu einer Untergruppe $PU(2,L')$ von $GL(2,L')$. Dabei geht $P\Omega(V)$, isomorph zu $\Omega(V)$, über in $PSL(2,L')$.*

(b) *Sei* $\operatorname{ind} V = 2$. *Dann ist $P\Omega(V) = \Omega(V)/\{1,-1\}$ isomorph zu $PSL(2,L) \times PSL(2,L)$.*

Beweis. 1. Sei N, M ein hyperbolisches Paar in V. Wir wählen eine orthogonale Basis von V der Form $E_1 = N + M/2$, $E_2 = N - M/2$, E_3, E_4. Der 3-dimensionale nichtisotrope Unterraum $W = \langle E_1, E_2, E_3 \rangle$ hat den Index 1. Wir wählen in $C^+(W)$, wie beim Beweis von Theorem 5 (ii), als Basiselemente $1, i_1 = E_2 \circ E_3$, $i_2 = E_3 \circ E_1$, $i_3 = E_1 \circ E_2$. Setze $E_1 \circ E_2 \circ E_3 \circ E_4 = e_V$. Wir haben $\bar{e}_V = e_V$. Für $e_V \circ e_V = e_V \circ \bar{e}_V = E_1{}^2E_2{}^2E_3{}^2E_4{}^4 = -E_3{}^2E_4{}^2$ schreiben wir Δ. Das Zentrum von $C^+(V)$, $Z^+(V)$, ist $L + e_VL$. Damit können wir $C^+(V)$ in folgender Weise als Tensorprodukt darstellen:

$$C^+(V) = C^+(W) \otimes Z^+(V). \tag{27}$$

2. Sei jetzt $\operatorname{ind} V = \operatorname{ind} g_I V = 1$. Da $\operatorname{ind}\langle E_1, E_2\rangle = 1$, ist dann $\operatorname{ind}\langle E_3, E_4\rangle = \operatorname{ind} g_I\langle E_3, E_4\rangle = 0$, das heisst nach Satz 16: $g_I(-E_3^2E_4^2) = g_I\Delta$ ist nicht Quadrat in L/I, also auch $\theta(-1) \neq L^{*2}$ und folglich Zentrum $\Omega(V) = \{1\}$. $Z^+(V) = L + e_V L$ ist ein lokaler Ring L' mit grösstem Ideal $I' = I + e_V I$. Aus (27) folgt daher

$$C^+(V) = C^+(W) \otimes L' = C^+(W \otimes L') = C^+(W') \tag{28}$$

wobei $W' = W \otimes L'$ ein 3-dimensionaler Raum vom Index 1 über L' ist.

Nach Satz 17 besteht $D(V)$ aus denjenigen $\alpha \in C^+(V)$, für die $\alpha \circ \bar{\alpha} \in L^*$. Diese α, aufgefasst als Elemente von $C^+(W')$, machen eine Untergruppe $D'(W')$ von $D(W')$ aus, wobei $D(W')$, nach Satz 17, aus den $\alpha \in C^+(W')$ mit $\alpha \circ \bar{\alpha} \in L'^*$ besteht. Es ist $D'(W') \cap L'^* = \{L^*, e_V L^*\}$. Aus (19) ergibt sich $s(e_V) = -1 \in \boldsymbol{SO}(V)$. Mit (21) ergibt sich also: $\boldsymbol{PSO}(V) = \boldsymbol{SO}(V)/\{1, -1\}$ ist isomorph zu $D(V)/\{L^*, e_V L^*\} = D'(W')/(D'(W') \cap L'^*)$ und dies ist isomorph zu einer Untergruppe $\boldsymbol{O}''(W')$ von $\boldsymbol{SO}(W')$.

Nach Satz 17 besteht $D_0(W')$ aus den $\alpha \in C^+(W') = C^+(V)$ mit $\alpha \circ \bar{\alpha} = 1$, und das sind gleichzeitig die Elemente von $D_0(V)$, d. h., $D_0(W') = D_0(V)$. Da $D_0(W') \subset D'(W')$ und $D_0(W') \cap L'^* = \{1, -1\}$, folgt mit (23), da $\boldsymbol{O}'(V) = \Omega(V)$ und $\boldsymbol{O}'(W') = \Omega(W')$: $\Omega(V)$ ist isomorph zu $D_0(V)/\{1, -1\} = D_0(W')/\{1, -1\}$, isomorph zu $\Omega(W')$. Bei dem Isomorphismus von $\boldsymbol{PSO}(V)$ auf $\boldsymbol{O}''(W')$ geht also die Untergruppe $P\Omega(V)$ (die wegen Zentrum $\Omega(V) = \{1\}$ isomorph ist zu $\Omega(V)$) über in $\Omega(W')$, wir haben also: $\Omega(W') \subset \boldsymbol{O}''(W') \subset \boldsymbol{SO}(W')$.

Nach Theorem 5 (ii) ist $\boldsymbol{SO}(W')$ isomorph zu $PGL(2, L')$; dabei geht $\Omega(W')$ über in $PSL(2, L')$. Also geht $\boldsymbol{O}''(W')$ über in eine Gruppe $PU(2, L')$, die zwischen $PSL(2, L')$ und $PGL(2, L')$ liegt.

3. Sei $\operatorname{ind} V = 2$. Nach Folgerung 2 zu Theorem 1 ist dann $V = P_1 \perp P_2$, wo P_1 und P_2 hyperbolische Ebenen sind. Wir können also in V eine orthogonale Basis E_i, $1 \leqq i \leqq 4$, so wählen, dass $E_1^2E_2^2E_3^2E_4^2 = 1$. In $Z^+(V) = L + e_V L$ ist also $e_V \circ e_V = 1$. Setze $f = (1 + e_V)/2$, $f' = (1 - e_V)/2$. Damit wird $Z^+(V) = fL + f'L$ und, mit (30), $C^+(V) = fC^+(W) + f'C^+(W)$, isomorph zu $C^+(W) \times C^+(W)$. Dabei geht ein Element $c \in L \subset Z^+(V)$ über in das Element $(c, c) \in C^+(W) \times C^+(W)$ und ein Element $e_V c \in Z^+(V)$ geht über in $(c, -c) \in C^+(W) \times C^+(W)$. Da $\Omega(V) = \boldsymbol{O}'(V)$, $\Omega(W) = \boldsymbol{O}'(W)$, und $s(e_V) = -1 \in \boldsymbol{SO}(V)$, haben wir mit (23):

$$P\Omega(V) = \Omega(V)/\text{Zentrum}\,\Omega(V) = \Omega(V)/\{1, -1\}$$

ist isomorph zu $D_0(V)/\{1, -1, e_V, -e_V\}$, isomorph zu $D_0(W)/\{1, -1\}$

$\times D_0(W)/\{1,-1\}$ isomorph zu $\Omega(W)\times\Omega(W)$ und dies ist, nach Theorem 5 (ii), isomorph zu $PSL(2,L)\times PSL(2,L)$.

ERGÄNZUNG ZU THEOREM 5 (iii, a). *Sei J ein Ideal in I. Bei dem Isomorphismus von $P\boldsymbol{SO}(V)$ auf $PU(2,L')$ geht die Untergruppe $P\Omega(V,J)$ $(=\Omega(V,J)/(\Omega(V,J)\cap \text{Zentrum}\,\boldsymbol{SO}(V))$, isomorph $\Omega(V,J))$ über in die Untergruppe $PSC(2,L',J')$ von $PU(2,L')$, mit $J'=J\otimes L'=J+e_VJ$.*

Beweis. Nach der Folgerung (i) zu Theorem 4 ist $\Omega(V,J)=\text{Kern}(h_J\colon \Omega(V)\to\Omega(g_JV))$. Andererseits ist (siehe Anhang)

$$PSC(2,L,J')=\text{Kern}(h_{J'}\colon PSL(2,L')\to PSL(2,L'/J')).$$

Da bei dem Isomorphismus von $\boldsymbol{SO}(V)$ auf $PU(2,L')$ $\Omega(V)$ übergeht in $PSL(2,L')$ und wegen (28) dem Ideal J das Ideal $J'=J\otimes L'$ entspricht, ergibt sich die Behauptung.

5. Die Struktur von $\boldsymbol{SO}(V)$ für ind $V\geqq 1$, dim $V\geqq 3$. Theorem 6.

5.1. *Die Ordnung einer Gruppe und deren Erzeugung.* Sei A ein Vektor in V mit $g_IA\neq 0$. Sei $\sigma\in\boldsymbol{O}(V)$. Unter der *Ordnung von σ bezüglich A, $o(\sigma,A)$,* verstehen wir das kleinste Ideal J in L so, dass $g_J\sigma A=\pm g_JA$, das heisst, $h_J\sigma\,|\langle g_JA\rangle=\pm 1$.

SATZ 18. (i) *Sei $\sigma\in\boldsymbol{O}(V)$ und sei A ein nichtisotroper Vektor von V. Setze $\langle A\rangle^0=H$. Sei E_j, $2\leqq j\leqq n=\dim V$, eine Basis von H. Wenn $\sigma A=Aa+\sum E_ja_j$, so ist $o(\sigma,A)$ gleich dem von den a_j, $2\leqq j\leqq n$, erzeugten Ideal $(a_2,\cdots,a_n)$.*

(ii) *Sei $\dim V\geqq 3$. Sei $\sigma\in\boldsymbol{O}(V)$. $o(\sigma)$ wird erzeugt von den Idealen $o(\sigma,A)$, wo A alle nichtisotropen Vektoren von V durchläuft.*

Beweis. 1. Beweis von (i). Setze $o(\sigma,A)=J$ und $(a_2,\cdots,a_n)=K$. Dann ist $h_K\sigma g_KA=g_K\sigma A=g_KAa$, und da $h_K\sigma\in\boldsymbol{SO}(g_KV)$, ist $g_Ka=\pm 1$, also $K\supset J$. Da $g_J(\sigma A-A)=0$ oder $g_J(\sigma A+A)=0$, ist $g_J(\sum E_ja_j)=0$, also $K\subset J$.

2. Beweis von (ii). Wir setzen $o(\sigma)=K$. Mit J bezeichnen wir das von den $o(\sigma,A)$ erzeugte Ideal, wo A alle nichtisotropen Vektoren durchläuft. Wegen $h_K\sigma=\pm 1$ haben wir $g_K\sigma A=\pm g_KA$, also $o(\sigma,A)\subset K$ für alle A, also $J\subset K$. Andererseits ist, für jedes nichtisotrope A, $h_J\sigma g_JA=g_J\sigma A=g_JA$, das heisst, $h_J\sigma$ lässt alle nichtisotropen Geraden in g_JV fest. Dann folgt nach Satz 9 $h_J\sigma=\pm 1$, also $J\supset K$.

Satz 19. *Sei* $\operatorname{ind} V \geqq 1$. *Sei* $\dim V = 4$ *und* $L/I \neq \mathbf{F}_3$ *oder sei* $\dim V \geqq 5$. *Sei* π *ein Element von* $\mathbf{SO}(V)$ *und sei* G *die von* π *erzeugte, unter* $\Omega(V)$ *invariante Untergruppe von* $\mathbf{SO}(V)$. *Dann gilt: Wenn* $A \in V$ *nichtisotrop ist, so ist* $o(\pi, A)$ *enthalten in einem Ideal, das erzeugt wird von Elementen* b *mit folgender Eigenschaft: Das von* b *erzeugte Ideal* (b) *kann dargestellt werden als* $(b) = o(\rho, B)$ *mit* $\rho \in G$ *und* B *nichtistrop.*

Beweis. 1. Sei A ein nichtisotroper Vektor. Sei E_j, $2 \leqq j \leqq n = \dim V$, eine orthogonale Basis von $H = \langle A \rangle^0$. Setze

$$\pi A = Aa + \sum E_j a_j. \tag{29}$$

Nach Satz 18 wird $o(\pi, A)$ erzeugt von den Elementen a_j, $2 \leqq j \leqq n$. Falls $o(\pi, A) = (1) = L$, so wählen wir $\rho = \pi$ und $B = A$. Wir nehmen daher jetzt an: $o(\pi, A) \subset I$. Es genügt zu zeigen, dass a_2 enthalten ist in einem Ideal (b_2, b'_2), dessen Erzeugende b_2, b'_2 die im Satz geforderte Eigenschaft haben.

2. Sei $L/I \neq \mathbf{F}_3$. Wir wählen in der nichtisotropen Ebene $P = \langle E_2, E_3 \rangle$ ein Element $\kappa \in \mathbf{SO}(P)$ so, dass $g_I \kappa^2 \neq 1$, vgl. Satz 12 (iii). Es ist $\theta(\kappa^2) = L^{*2}$. Wir setzen κ^2 durch die Identität auf P^0 fort und bezeichnen dieses Element mit λ. Wegen $\theta(\lambda) \in L^{*2}$ ist nach Theorem 4 (i) $\lambda \in \Omega(V)$. Daher $\tau = \lambda \pi \lambda^{-1} \pi^{-1} \in G$. Wir finden

$$\tau \pi A = \lambda \pi A = \pi A + (\lambda E_2 - E_2) a_2 + (\lambda E_3 - E_3) a_3. \tag{30}$$

Da $h_I \lambda \mid g_I P = h_I \kappa^2$ nicht die Identität ist und nicht die Symmetrie an einer Geraden, ist $\langle \lambda E_2 - E_2, \lambda E_3 - E_3 \rangle = \langle E_2, E_3 \rangle$ eine nichtisotrope Ebene. Da $o(\pi, A) \subset I$, ist $g_I B = g_I A$ orthogonal zu $g_I \langle E_2, E_3 \rangle$. Folglich erzeugen die Vektoren

$$B = \pi A, \quad E'_2 = \lambda E_2 - E_2, \quad E'_3 = \lambda E_3 - E_3 \tag{31}$$

einen nichtisotropen 3-dimensionalen Raum W. Wir setzen

$$F'_2 = E'_2 - B(BE'_2)/B^2, \quad F'_3 = E'_3 - B(BE'_3)/B^2. \tag{32}$$

Die Vektoren F'_2, F'_3 sind orthogonal zu B in W und spannen eine nichtisotrope Ebene auf. Es gibt also in $\langle F'_2, F'_3 \rangle$ eine orthogonale Basis F_2, F_3. Damit erhalten wir aus (30)

$$\tau B = \lambda B = Bb + F_2 b_2 + F_3 b'_2 \tag{33}$$

mit $(b_2, b'_2) = (a_2, a_3)$, also insbesondere $a_2 \in (b_2, b'_2)$.

Wir ergänzen B, F_2, F_3 durch eine orthogonale Basis F_k, $4 \leqq k \leqq n$, von W^0 zu einer Basis von V. Es gibt wiederum $\mu \in \Omega(V)$ so, dass μ auf $\langle F_2, F_4 \rangle^0$

die Identität ist, während $\mu F_2 - F_2$ und $\mu F_4 - F_4$ eine Basis von $\langle F_2, F_4\rangle$ sind. Dann gehört auch $\rho = \mu\tau\mu^{-1}\tau^{-1}$ zu G. Wir finden, da die Gleichung (33) an die Stelle von (29) getreten ist, als Gegenstück zu (30)

$$(34) \qquad \rho\tau B = \mu\tau B = \tau B + (\mu F_2 - F_2) b_2.$$

Damit wird $(b_2) = o(\rho, \tau B)$.

Wir wählen jetzt $\gamma \in \Omega(V)$ so, dass γ auf $\langle F_3, F_4\rangle^0$ die Identität ist, während $\gamma F_3 - F_3$ und $\gamma F_4 - F_4$ eine Basis von $\langle F_3, F_4\rangle$ bilden. Dann gehört auch $\chi = \gamma\tau\gamma^{-1}\tau^{-1}$ zu G, und wir haben

$$(35) \qquad \chi\tau B = \gamma\tau B = \tau B + (\gamma F_3 - F_3) b'_2.$$

Also $(b'_2) = o(\chi, \tau B)$.

3. Sei jetzt $L/I = \boldsymbol{F}_3$. Nach Voraussetzung ist dann $n = \dim V \geqq 5$. Wir unterscheiden drei Fälle:

(i) $\operatorname{ind} g_I\langle E_2, E_3\rangle = 0$. Dann können wir zunächst schliessen wie in 2. Nach Satz 12 (iii) gibt es $\kappa \subset \boldsymbol{SO}(\langle E_2, E_3\rangle)$ so, dass $g_I\kappa$ nicht eine Involution ist. Wir setzen $\kappa^2 \mid \langle E_2, E_3\rangle \perp 1 \mid \langle E_2, E_3\rangle^0 = \lambda$. Dann $\lambda\pi\lambda^{-1}\pi^{-1} = \tau \in G$ und es gilt (33). In $W^0 = \langle B, F_2, F_3\rangle^0$ gibt es einen Vektor F_4 mit $g_I F_4^2 = g_I F_2^2$. Denn $\dim g_I W^0 = n - 3 \geqq 2$. Damit ist $\langle F_2, F_4\rangle$ nichtisotrop und $\operatorname{ind} g_I\langle F_2, F_4\rangle = 0$. Auf die Ebene $\langle F_2, F_4\rangle$ können wir die Überlegungen aus 2. anwenden und finden, wie in 2., $\rho \in G$ so, dass $(b_2) = o(\rho, \tau B)$. Ebenso lässt sich (b'_2) darstellen, und $a_2 \in (b_2, b'_2)$.

(ii) Sei $\operatorname{ind} g_I\langle E_2, E_3\rangle = 1$ und $\operatorname{ind} g_I\langle E_2, E_4\rangle = 0$. Wir lassen E_4 und a_4 an die Stelle von E_3 und a_3 treten und schiessen wie in (i).

(iii) Sei $\operatorname{ind} g_I\langle E_2, E_3\rangle = \operatorname{ind} g_I\langle E_2, E_4\rangle = 1$. Dann ist $\operatorname{ind} g_I\langle E_3, E_4\rangle = 0$. $\langle E_2, E_3 + E_4\rangle$ ist nichtisotrop und $\operatorname{ind} g_I\langle E_2, E_3 + E_4\rangle = 0$. Wir setzen $E'_3 = E_3 + E_4$, $E'_4 = E_3 c - E_4$ mit $c = E_4^2/E_3^2$. Aus (29) wird

$$\pi A = Aa + E_2 a_2 + E'_3 a'_3 + E'_4 a'_4 + \cdots.$$

Wegen $\operatorname{ind} g_I\langle E_2, E'_3\rangle = 0$ können wir wie in (i) schliessen.

Satz 20. *Sei* $\dim V \geqq 3$. *Sei* $\sigma \in \boldsymbol{O}(V)$ *von der Form* $\sigma = \tau_{\pi A}\tau_A$, *also* $\sigma \in \boldsymbol{SO}(V)$ *und* A *nichtisotrop. Dann ist* $o(\sigma) = o(\pi, A)$.

Beweis. Setze $o(\sigma) = J$ und $o(\pi, A) = K$. Aus $h_K \tau_{\pi A} = \tau_{g_K \pi A} = \tau_{\pm g_K A}$ folgt $h_K \tau_{\pi A}\tau_A = 1$, also $K \supset J$. Andererseits folgt aus $h_J \sigma = +1$, d. h., $\tau_{g_J \pi A}\tau_{g_J A} = 1$, dass $g_J \pi A = h_J \pi g_J A$ und $g_J A$ linear abhängig sind, also $J \supset K$.

5.2. *Invariante Gruppen* G, *die erzeugt werden von Elementen der Form* $\sigma = \tau_{\pi A}\tau_A$, *wo* $o(\sigma)$ *ein Hauptideal ist.*

SATZ 21. *Sei* $\dim V \geqq 4$. *Sei A ein nichtisotroper Vektor* $\sigma \in \boldsymbol{SO}(V)$ *so, dass A und* σA *einem 2-dimensionalen Untermodul P angehören, d. h., P ist direkter Summand von V der Dimension 2, aber nicht notwendig Unterraum. Sei* $g_I P$ *isotrop in* $g_I V$. *Dann gibt es in der von* σ *erzeugten, unter* $\Omega(V)$ *invarianten Gruppe G in* $\boldsymbol{SO}(V)$ *ein Element* λ *so, dass* A, λA *einer nichtisotropen Ebene angehören und* $o(\lambda, A) = o(\sigma, A)$.

Beweis. 1. Nach Voraussetzung enthält $g_I P$ ein Radikal $\neq 0$. Da $g_I A$ nichtisotrop ist und zu $g_I P$ gehört, ist $\dim \operatorname{rad} g_I P = 1$. Sei N ein Vektor in P so, dass $\langle g_I N \rangle = \operatorname{rad} g_I P$. A und N sind eine Basis von P.

2. Sei $\sigma A = Aa + Nu$. Aus $a \in I$ folgt $g_I \sigma A = g_I N u$ isotrop—ein Widerspruch. Also $a \in L^*$. Für $1/a$ schreiben wir a und für $-u/a$ schreiben wir u. Damit wird

$$A = \sigma A a + N u. \tag{36}$$

3. Wir bezeichnen die Elemente von $g_I V$ mit einem Querstrich. Setze $\overline{\langle \sigma A \rangle}^0 = \bar{H}$. Wegen $\bar{N} \in \bar{H}$ gibt es in $\bar{H}$ einen isotropen Vektor $\bar{M}$ so, dass $\bar{N}$, $\bar{M}$ ein hyperbolisches Paar bilden. Da $\dim \bar{H} = n - 1 \geqq 3 > \dim \langle \bar{N} \rangle + \dim \operatorname{rad} \langle \bar{N} \rangle = 2$, gibt es nach der Ergänzung zu Theorem 1 ein $\bar{\sigma} \in \boldsymbol{SO}(\bar{H})$ mit $\bar{\sigma}\bar{N} = \bar{M}$. Es sei $\theta(\bar{\sigma}) = \bar{b}\bar{L}^{*2}$. Wir definieren $\bar{\rho} \in \boldsymbol{SO}(\langle \bar{N}, \bar{M} \rangle)$ durch $\bar{\rho}\bar{M} = \bar{M}\bar{b}$, $\bar{\rho}\bar{N} = \bar{N}/\bar{b}$. Dann ist für $\bar{\lambda} = \bar{\rho}\bar{\sigma}$: $\theta(\bar{\lambda}) = \bar{L}^{*2}$, also, nach Theorem 4 (i), $\bar{\lambda} \in \Omega(\bar{H})$.

Sei λ ein Urbild von $\bar{\lambda}$ in $\Omega(H)$, $H = \langle \sigma A \rangle^0$. Ein solches Urbild existiert, nach Folgerung 3 zu Theorem 3. Damit erhalten wir mit (36): $\lambda A = \lambda \sigma A a + \lambda N u = \sigma A a + \lambda N u = A + (\lambda N - N) u$. A und $\lambda N - N$ erzeugen eine nichtisotrope Ebene. Denn $\bar{A}$ und $\bar{\lambda}\bar{N} - \bar{N} = \bar{M}\bar{b} - \bar{N}$ sind nichtisotrop und aus $\bar{A}\bar{r} = (\bar{M}\bar{b} - \bar{N})\bar{s}$ folgt $\bar{A}\bar{r} + \bar{N}\bar{s} = \bar{M}\bar{b}\bar{s}$, also $\bar{A}^2\bar{r}^2 = \bar{M}^2\bar{b}^2\bar{s}^2 = 0$, also $\bar{r} = \bar{s} = 0$.

SATZ 22. *Sei* $\dim V \geqq 3$, $\operatorname{ind} V \geqq 1$. *Seien A, B zwei nichtisotrope Vektoren in V, die einem 2-dimensionalen Untermodul P angehören. Dann gibt es einen 3-dimensionalen nichtisotropen Unterraum U mit* $\operatorname{ind} U = 1$, *der P enthält.*

Beweis. 1. Wir betrachten zunächst den Fall, dass P eine nichtisotrope Ebene ist. Dann ist auch P^0 nichtisotrop. Wir behaupten: Es gibt einen isotropen Vektor N so, dass $g_I N$ weder zu $g_I P$ noch zu $g_I P^0$ gehört. Wenn wir das gezeigt haben, dann erklären wir U durch $U = \langle P, N \rangle$. Wäre nämlich für jeden isotropen Vektor N $g_I N \in g_I P$ oder $g_I N \in g_I P^0$, so würde die Symmetrie $\sigma = 1 \mid P \perp -1 \mid P^0$ an P die Voraussetzungen von Satz 8 erfüllen mit $J = I$, also $h_I \sigma = \pm 1$, ein Widerspruch.

2. Es sei jetzt P nicht nichtisotrop, das heisst, g_IP sei isotrop. Da g_IP den nichtisotropen Vektor g_IA enthält, ist $\dim \operatorname{rad} g_IP = 1$. Wir wählen $N \in P$ so, dass $\langle g_IN\rangle = \operatorname{rad} g_IP$. Dann ist A, N eine Basis von P. Wir behaupten: Es gibt ein M isotrop in V so, dass $\langle g_IM\rangle$ komplementär ist zu $\langle g_IN\rangle^0$ in g_IV, also $NM \in L^*$. Wenn das gezeigt ist, erklären wir U durch $U = \langle A, N, M\rangle$.

Angenommen, für alle isotropen Vektoren M von V gilt: $g_IM \in \langle g_IN\rangle^0$. Sei N', M' ein hyperbolisches Paar in V. Dann also g_IN' und g_IM' in $\langle g_IN\rangle^0$. Setze $Q = \langle N', M'\rangle$. Q^0 ist nichtisotrop und enthält Vektoren D so, dass g_ID nicht zu $\langle g_IN\rangle^0$ gehört. Unter diesen D gibt es auch einen nichtisotropen Vektor. Denn es können nicht alle Vektoren des $(n-2)$-dimensionalen nichtisotropen Raumes g_IQ^0, die komplementär sind zu dem darin enthaltenen $(n-3)$-dimensionalen Unterraum $\langle g_IN\rangle^0 \cap g_IQ^0$, isotrop sein. Mit einem solchen nichtisotropen D ist dann $M = N' - M'D^2/2 + D$ isotrop und so, dass $NM \in L^*$.

Satz 23. *Sei* $L/I = \boldsymbol{F}_3$, $\dim V \geqq 5$. *Sei* U *ein 3-dimensionaler nichtisotroper Unterraum von* V *mit* $\operatorname{ind} U = 1$. *Dann gibt es einen 4-dimensionalen nichtisotropen Unterraum* W *in* V, *der* U *enthält und so, dass* $\operatorname{ind} W = \operatorname{ind} g_IW = 1$.

Beweis. In U gibt es ein hyperbolisches Paar N, M. Sei B ein zu $\langle N, M\rangle$ orthogonaler, nichtisotroper Vektor in U. Damit wird $U = \langle N, M, B\rangle$. U^0 ist nichtisotrop und $\dim U^0 = n - 3 \geqq 2$. Daher gibt es in g_IU^0 einen Vektor $\bar{C}$ mit $\bar{C}^2 = g_IB^2$. Wähle $C \in U^0$ mit $g_IC = \bar{C}$. $W = \langle N, M, B, C\rangle$ hat dann die geforderten Eigenschaften.

Satz 24. *Sei* $\dim V \geqq 5$, $\operatorname{ind} V \geqq 1$. *Sei* $\sigma = \tau_{\pi A}\tau_A \in \boldsymbol{SO}(V)$ *so, dass* $o(\sigma) = (u)$ *ein Hauptideal ist. Dann ist die von* σ *erzeugte, unter* $\Omega(V)$ *invariante Untergruppe* G *von* $\boldsymbol{SO}(V)$ *gleich* $\Omega(V, o(\sigma)) = \Omega(V, (u))$.

Beweis. 1. In den Abschnitten 2. bis 4. setzen wir voraus $L/I \neq \boldsymbol{F}_3$, in 5. ist $L/I = \boldsymbol{F}_3$.

2. Nach Satz 20 ist $o(\pi, A) = (u)$, also $\pi A = Aa + Bu$, wo g_IA und g_IB linear unabhängig sind in g_IV. A und πA gehören also dem 2-dimensionalen Untermodul $\langle A, B\rangle$ an und nach Satz 22 einem 3-dimensionalen nichtisotropen Unterraum U mit $\operatorname{ind} U = 1$. Wegen $\sigma \mid U^0 = 1$ können wir σ als Element von $\boldsymbol{SO}(U)$ auffassen. Wir haben, vgl. (13), $\sigma = \tau_{\pi A}\tau_A = (\tau_{\pi A + \epsilon A}\tau_A)^2$ mit $\epsilon = 1$ oder $= -1$. Nach Theorem 3 ist σ also ein Element von $\Omega(U, (u))$ der Ordnung (u). Nach Theorem 5 (ii) und der Ergänzung ist $G \cap \Omega(U, (u))$ isomorph eined unter $PSL(2, L)$ invarianten Untergruppe G'

von $PGL(2, L)$, die ein Element der Ordnung (u) enthält (nämlich das Bild von $\sigma \in G \cap \Omega(U, (u))$) und die enthalten ist in $PSC(2, L, (u))$ (*da* $\Omega(U, (u))$ übergeht in $PSC(2, L, (u))$). Nach dem Struktursatz von $PGL(2, L)$ (siehe Anhang) ist daher $G' = PSC(2, L, (u))$, also $G \cap \Omega(U, (u)) = \Omega(U, (u))$.

3. Sei U' ein beliebiger nichtisotroper Unterraum von V mit $\dim U' = 3$ und $\operatorname{ind} U' = 1$. U' enthält ein hyperbolisches Paar N', M'. Insbesondere enthält der Raum U aus 2. ein hyperbolisches Paar N, M. Die hyperbolischen Ebenen $P = \langle N, M \rangle$ und $P' = \langle N', M' \rangle$ sind isometrisch. Nach der Ergänzung zu Theorem 1 gibt es $\sigma \in \boldsymbol{SO}(V)$ mit $\sigma P = P'$. In $\boldsymbol{SO}(P')$ gibt es nach Theorem 4 (ii) ein ρ so, dass $\theta(\rho) = \theta(\sigma)$, also $\theta(\rho\sigma) = L^{*2}$, das heisst nach Theorem 4(i): $\lambda = \rho\sigma \in \Omega(V)$. Es ist $\lambda P = P'$. Da G invariant ist unter $\Omega(V)$, enthält G mit der Gruppe $\Omega(P, (u)) \subset \Omega(U, u))$ auch $\lambda\Omega(P, (u))\lambda^{-1} = \Omega(P', (u))$. In $\Omega(P', (u))$ gibt es ein Element σ' der Ordnung (u), zum Beispiel $\sigma' N' = N'(1+u)^2$, $\sigma' M' = M'/(1+u)^2$. Da $\sigma' \in \Omega(P', (u)) \subset G \cap \Omega(U', (u))$, schliessen wir wie in 2.: $\Omega(U', (u)) \subset G$.

4. $\Omega(V, (u))$ wird erzeugt von Elementen der Form $\rho\tau_B\rho^{-1}\tau_B = \tau_{\rho B}\tau_B$ mit $\rho \in \boldsymbol{SO}(V, (u))$, also $o(\tau_{\rho B}\tau_B) \subset (u)$. Falls $o(\tau_{\rho B}\tau_B) = (u)$, so gehören B und ρB einem 2-dimensionalen Untermodul an, also nach Satz 22 einem nichtisotropen Unterraum U' mit $\dim U' = 3$ und $\operatorname{ind} U' = 1$. Nach 3. ist dann $\tau_{\rho B}\tau_B \in \Omega(U', (u)) \subset G$. Falls dagegen $o(\tau_{\rho B}\tau_B) \neq (u)$, so wählen wir $\kappa \in \boldsymbol{O}(V)$ derart, dass $o(\tau_{\kappa B}\tau_B) = (u)$ (Wir können etwa, falls $(u) \subset I$, $\kappa = \tau_{B+Cu}$ wählen, wo C ein zu B orthogonaler, nichtisotroper Vektor ist). Dann ist auch $o(\tau_{\rho B}\tau_{\kappa\rho^{-1}\rho B}) = (u)$, und mit $\tau_{\rho B}\tau_{\kappa B}$ und $\tau_{\kappa B}\tau_B$ gehört auch $\tau_{\rho B}\tau_{\kappa B}\tau_{\kappa B}\tau_B = \tau_{\rho B}\tau_B$ zu G. G enthält also alle Erzeugenden von $\Omega(V, (u))$ und wird erzeugt von einem Element σ von $\Omega(V, (u))$, also $G = \Omega(V, (u))$.

5. Sei jetzt $L/I = \boldsymbol{F}_3$. Zunächst schiessen wir wieder, wie in 2., auf Grund von Satz 20 und Satz 22, dass A und πA enthalten sind in einem nichtisotropen Unterraum U mit $\dim U = 3$, $\operatorname{ind} U = 1$. Nach Satz 23 ist U enthalten in einem Unterraum W mit $\dim W = 4$, $\operatorname{ind} W = \operatorname{ind} g_I W = 1$, so dass wir σ auffassen können als Element der Ordnung (u) in $G \cap \Omega(W, (u))$. Nach Theorem 5 (iii) und der Ergänzung ist $G \cap \Omega(W, (u))$, aufgefasst als unter $\Omega(W)$ invariante Untergruppe von $\boldsymbol{SO}(W)$, isomorph einer unter $PSL(2, L')$ invarianten Untergruppe G' von $PU(2, L') \subset PGL(2, L')$. G' enthält ein Element der Ordnung (u'), wo $(u') = uL'$ das von u in L' erzeugte Ideal bezeichnet, nämlich das Bild von $\sigma \in G \cap \Omega(W, (u))$, und da $\Omega(W, (u))$ übergeht in $PSC(2, L', (u'))$, ist G' enthalten in $PSC(2, L', (u'))$, das heisst nach dem Struktursatz von $PGL(2, L')$ (siehe Anhang): $G' = PSC(2, L', (u'))$, also $G \cap \Omega(W, (u)) = \Omega(W, (u))$.

Jetzt können wir weiterschliessen wie in 3. und 4.: $\Omega(V, (u))$ wird erzeugt von Elementen $\tau_{\rho B}\tau_B$ mit $o(\rho, B) = (u)$, und, wie wir in 4. zeigten, können wir uns auf den Fall $o(\tau_{\rho B}\tau_B) = o(\rho, B) = (u)$ beschränken. B und ρB gehören dann einem nichtisotropen Unterraum U' an mit $\dim U' = 3$, $\operatorname{ind} U' = 1$, und U' ist, nach Satz 23, enthalten in einem nichtisotropen Unterraum W' mit $\dim W' = 4$ und $\operatorname{ind} W' = \operatorname{ind} g_I W' = 1$. Mit Hilfe von hyperbolischen Ebenen $P \subset W$ und $P' \subset W'$ schliessen wir dann wieder, dass $G \cap \Omega(W')$ ein Element der Ordnung (u) enthält, also, wie oben, $\tau_{\rho B}\tau_B \in \Omega(W', (u)) \subset G$.

5.3. *Die Zurückführung des Falles einer beliebigen invarianten Untergruppe G auf den in 5.2 betrachteten Fall.*

Satz 25. *Sei $\operatorname{ind} V \geqq 1$, $\dim V \geqq 5$. Sei $\sigma \in \boldsymbol{SO}(V)$ von der Form $\tau_{\pi A}\tau_A$. Die von σ erzeugte, unter $\Omega(V)$ invariante Untergruppe G von $\boldsymbol{SO}(V)$ enthält die Gruppe $\Omega(V, o(\sigma))$.*

Beweis. 1. Nach Satz 20 ist $o(\sigma) = o(\pi, A)$. Sei E_j, $2 \leqq j \leqq n = \dim V$, eine orthogonale Basis von $H = \langle A \rangle^0$. Sei $\pi A = Aa + \sum E_j a_j$. Nach Satz 18 (i) wird $o(\sigma) = o(\pi, A)$ erzeugt von den a_j, $2 \leqq j \leqq n$. Falls $o(\sigma) = (1) = L$, so haben wir den in Satz 24 betrachteten Fall vor uns. Wir nehmen daher an: $o(\sigma) \subset I$, also $(a_j) \subset I$ für alle j, $2 \leqq j \leqq n$. Der Satz ist bewiesen, wenn wir zeigen, dass für jedes j, $2 \leqq j \leqq n$, Elemente b_j, b'_j existieren so, dass $a_j \in (b_j, b'_j)$ und $\Omega(V, (b_j)) \subset G$ und $\Omega(V, (b'_j)) \subset G$. Wir führen diesen Nachweis für den Fall $j = 2$ und schliessen uns dabei eng an den Beweis von Satz 19 an.

2. Sei $L/I \neq \boldsymbol{F}_3$. Wir wählen $\lambda \in \Omega(V)$ wie l. c. 2. Wegen $\lambda A = A$ haben wir $\tau = \lambda\sigma\lambda^{-1}\sigma^{-1} = \lambda\tau_{\pi A}\tau_A\lambda^{-1}\tau_A\tau_{\pi A} = \tau_{\lambda\pi A}\tau_{\pi A} \in G$. Für $\lambda\pi A$ haben wir den Ausdruck (30), also $o(\tau) = o(\lambda, \pi A) = (a_2, a_3)$. Wir setzen $\pi A = B$ und wählen in $W = \langle B, E_2, E_3 \rangle$ eine orthogonale Basis B, F_2, F_3 wie l. c., mit Hilfe von (31) und (32). Für $\lambda\pi A = \lambda B$ haben wir den Ausdruck (33), mit $a_2 \in (b_2, b'_2)$. Wir wählen $\mu \in \Omega(V)$ wie l. c. Mit $\mu\pi A = \pi A$ haben wir $\rho = \mu\tau\mu^{-1}\tau^{-1} = \mu\tau_{\lambda\pi A}\tau_{\pi A}\mu^{-1}\tau_{\pi A}\tau_{\lambda\pi A} = \tau_{\mu\lambda\pi A}\tau_{\lambda\pi A} \in G$. $\mu\lambda\pi A$ ist, mit $\lambda\pi A = \tau B$, gegeben durch (34), also $o(\rho) = o(\mu, \lambda\pi A) = (b_2)$. Aus Satz 24 folgt $\Omega(V, (b_2)) \subset G$. Wir wählen schiesslich $\gamma \in \Omega(V)$ wie l. c. und haben, mit $\gamma\pi A = \pi A$, $\chi = \gamma\tau\gamma^{-1}\tau^{-1} = \gamma\tau_{\lambda\pi A}\tau_{\pi A}\gamma^{-1}\tau_{\pi A}\tau_{\lambda\pi A} = \tau_{\gamma\lambda\pi A}\tau_{\lambda\pi A} \in G$. $\gamma\lambda\pi A$ ist, mit $\lambda\pi A = \tau B$, gegeben durch (35), also $o(\chi) = o(\gamma, \lambda\pi A) = (b'_2)$. Aus Satz 24 folgt wiederum $\Omega(V, (b'_2)) \subset G$.

3. Sei $L/I = \boldsymbol{F}_3$. Wie wir in Teil 3 des Beweis von Satz 19 gezeigt haben, lässt dieser Fall sich zurückführen auf den in 2. betrachteten Fall.

Satz 26. *Sei $\dim V = 3$ und $L/I \neq \boldsymbol{F}_3$ oder sei $\dim V \geqq 4$. Sei J ein*

Ideal in I. Sei A ein nichtisotroper Vektor in V und sei $\sigma \in \boldsymbol{SO}(V)$ ein Element mit folgender Eigenschaft: $h_J\sigma g_J A = g_J A$ und, falls $B^2 = A^2$, $h_J\sigma g_J B = \pm g_J B$. Dann ist $h_J\sigma = 1$.

Beweis. 1. Setze $\langle A\rangle^0 = H$. H besitzt eine Basis aus nichtisotropen Vektoren. Sei E ein solcher Vektor. Setze $\langle A, E\rangle = P$. Wir wollen zeigen, dass $h_J\sigma \mid g_J P = 1$, also $h_J\sigma g_J E = g_J E$. Damit wird der Satz dann bewiesen sien. Wir unterscheiden drei Fälle.

2. L/I enthält wenigstens 6 Elemente oder $L/I = \boldsymbol{F}_5$ und $\operatorname{ind} g_I P = 0$. Unter diesen Voraussetzungen gibt es wenigstens 6 nichtisotrope Geraden in $g_I P$. Es gibt also eine Gerade in $g_I P$ so, dass die Symmetrie $\bar{\tau}$ an dieser Geraden einen Vektor $\bar{\tau} g_I A$ liefert, der zusammen mit $g_I A$ eine nichtorthogonale Basis von $g_I P$ bildet. Wir wählen $\tau \in \boldsymbol{O}(P)$ so, dass $h_I\tau = \bar{\tau}$. Setze $\tau A = B$. Wegen $B^2 = A^2$ haben wir $h_J\sigma g_J B = \pm g_J B$. Aus $h_J\sigma g_J B = -g_J B$ ergibt sich ein Widerspruch: Denn dann ist $g_J AB = 0$, also $g_I A$ und $g_I B = h_I\tau g_I A$ bilden eine orthogonale Basis von $g_I P$, was ausgeschlossen war. Also $h_J\sigma g_J B = g_J B$, d. h., $h_J\sigma \mid g_J P = 1$.

3. $L/I = \boldsymbol{F}_5$ und $\operatorname{ind} g_I P = 1$. Also 3(i) $g_I A^2 + g_I E^2 = 0$ oder 3(ii) $g_I A^2 - g_I E^2 = 0$. Wir beschränken uns darauf, den Fall 3(i) zu diskutieren, das Fall 3(ii) wird ganz analog behandelt. Sei F ein weiteres Element der orthogonalen Basis von H. Dann ist 3(ij) $g_I E^2 + g_I F^2 \neq 0$ oder 3(ijj) $g_I E^2 - g_I F^2 \neq 0$. Im Fall 3(ij) sind $\langle A, E \pm F\rangle$ nichtisotrop und $\operatorname{ind} g_I\langle A, E \pm F\rangle = 0$, so dass nach 2. folgt: $h_J\sigma(g_J E \pm g_J F) = g_J E \pm g_J F$, also $h_J\sigma g_J E = g_J E$. Im Fall 3(ijj) sind $\langle A, E \pm 2F\rangle$ nichtisotrop und $\operatorname{ind} g_I\langle A, E \pm 2F\rangle = 0$, also, nach 2., $h_J\sigma(g_J E \pm 2g_J F) = g_J E \pm 2g_J F$, also $h_J\sigma g_J E = g_J E$.

4. Sei $L/I = \boldsymbol{F}_3$. Da $\dim P^0 = n - 2 \geqq 2$, gibt es $F \in P^0$ mit $g_I F^2 = -g_I E^2$. Setze $N = 2E + F$, $M = -E - F$. Dann wird $E = N + M$. $g_I N$ und $g_I M$ sind isotrop. Ferner $g_I(A + N)^2 = g_I A^2$. Es gibt also ein $\bar{\lambda} \in \boldsymbol{O}(g_I V)$ mit $\bar{\lambda} g_I A = g_I(A + N)$. Sei $\lambda \in \boldsymbol{O}(V)$ so, dass $h_I\lambda = \bar{\lambda}$. Dann ist $(\lambda A)^2 = A^2$, also $h_J\sigma g_J(\lambda A) = \pm g_J(\lambda A)$. Da $h_I\sigma g_I(\lambda A) = h_I\sigma g_I(A + N) = g_I A + h_I\sigma g_I N$, folgt $h_J\sigma g_J N = g_J N$. Ebenso ergibt sich $h_J\sigma g_J M = g_J M$ und daher auch $h_J\sigma g_J E = g_J E$.

SATZ 27. *Sei* $\operatorname{ind} V \geqq 1$, $\dim V \geqq 5$. *Wenn es zu einem $\sigma \in \boldsymbol{SO}(V)$ einen nichtisotropen Vektor A so gibt, dass $\sigma A = A$ ist, dann enthält die von σ erzeugte, unter $\Omega(V)$ invariante Untergruppe G von $\boldsymbol{SO}(V)$ die Gruppe $\Omega(V, o(\sigma))$.*

Beweis. 1. Wir betrachten das Ideal J, das erzeugt wird von den Idealen

$o(\sigma, B)$ wo B alle Vektoren mit $B^2 = A^2$ durchläuft. Wir behaupten: $J = o(\sigma)$. Wenn $J = L$, so steht das Gleichheitszeichen. Wir nehmen daher an: $J \subset I$. Das Element σ erfüllt dann die Voraussetzungen von Satz 26. Wir haben also $h_J\sigma = 1$, also $o(\sigma) \subset J$.

2. Sei B ein Vektor in V mit $B^2 = A^2$. Es gibt $\mu \in \boldsymbol{SO}(V)$ mit $\mu A = B$. Dann $\lambda = \tau_B \tau_A = \mu \tau_A \mu^{-1} \tau_A \in \Omega(V)$ und $\rho = \sigma\lambda\sigma^{-1}\lambda^{-1} = \sigma\tau_B\tau_A\sigma^{-1}\tau_A\tau_B = \tau_{\sigma B}\tau_B \in G$. Nach Satz 25 haben wir $\Omega(V, o(\sigma, B)) \subset G$. Mit 1. folgt jetzt die Behauptung.

Satz 28. *Sei* $\operatorname{ind} V \geqq 1$, $\dim V \geqq 5$. $\sigma \in \boldsymbol{SO}(V)$. *Die von* σ *erzeugte, unter* $\Omega(V)$ *invariante Untergruppe* G *von* $\boldsymbol{SO}(V)$ *enthält die Gruppe* $\Omega(V, o(\sigma))$.

Beweis. 1. Nach Satz 18 (ii) wird wird $o(\sigma)$ erzeugt von den Idealen $o(\sigma, A)$, wo A alle nichtisotropen Vektoren von V durchläuft. Wenn wir zeigen, dass $\Omega(V, o(\sigma, A)) \subset G$ für jedes solche Ideal $o(\sigma, A)$, dann ist der Satz beweisen.

Nach Satz 19 ist $o(\sigma, A)$ enthalten in einem Ideal, das erzeugt wird von Elementen u so, dass zu jedem u ein $\rho \in G$ und ein nichtisotroper Vektor B existieren mit $(u) = o(\rho, B)$. Der Satz ist bewiesen, wenn wir zeigen, dass $\Omega(V, (u)) \subset G$ für alle diese u.

Wir betrachten daher jetzt ein $\sigma \in \boldsymbol{SO}(V)$ und einen nichtisotropen Vektor A so, dass $o(\sigma, A) = (u)$ ein Hauptideal ist. Sei G die von σ erzeugte, unter $\Omega(V)$ invariante Untergruppe von $\boldsymbol{SO}(V)$. Der Satz ist bewiesen, wenn wir zeigen:

$$\Omega(V, (u)) \subset G. \tag{37}$$

2. Wegen $o(\sigma, A) = (u)$ gibt es einen zu A orthogonalen Vektor B so, dass $g_1 B \neq 0$ und

$$\sigma A = Aa + Bu. \tag{38}$$

Auf Grund von Satz 21 können wir annehmen, dass die Ebene $P = \langle A, B \rangle$ nichtisotrop ist, so dass A, B eine orthogonale Basis von P bilden. Wir wählen in dem nichtisotropen Raum P^0 eine orthogonale Basis E_k, $3 \leqq k \leqq n = \dim V$. Sei

$$\sigma B = Av + Bb + \sum E_k b_k, \qquad 3 \leqq k \leqq n. \tag{39}$$

Mit K bezeichnen wir das von den b_k, $3 \leqq k \leqq n$, erzeugte Ideal. Wir behaupten

$$\Omega(V, K) \subset G. \tag{40}$$

Dazu genügt es zu zeigen, dass $\Omega(V, (b_k)) \subset G$ für alle k, $3 \leqq k \leqq n$. Wir beweisen diese Inklusion für $k = 3$. Dazu wählen wir ein Element $\lambda \in \Omega(P^0)$

so, dass $g_I(\lambda E_3 - E_3) \neq 0$ ist Ein solches λ gibt es, da, wegen $\dim P^0 = n-2 \geqq 3$, E_3 enthalten ist einer nichtisotropen Eben Q von P^0 mit $\operatorname{ind} g_I Q = 0$. Nach Satz 12(iii) gibt es $\kappa \in \boldsymbol{O}(Q)$ mit $g_I \kappa^2 \neq 1$. Wir setzen $\lambda = \kappa^2 \mid Q \perp 1 \mid Q^0 \cap P^0$. Da $\theta(\kappa^2) = L^{*2}$, ist nach Theorem 4(i) $\kappa^2 \in \Omega(Q)$, also auch $\lambda \in \Omega(P^0)$, und da $g_I\lambda \mid g_I Q = g_I \kappa^2$ nicht die Symmetrie an der zu $g_I E_3$ orthogonalen Geraden in $g_I Q$ sein kann, ist $g_I(\lambda E_3 - E_3) \neq 0$.

Mit $\sigma \in G$ ist auch $\rho = \lambda\sigma\lambda^{-1}\sigma^{-1} \in G$. Auf Grund von (39) haben wir

$$\begin{aligned} &\rho\sigma A = \sigma A, \\ &\rho\sigma B = \sigma B + (\lambda E_3 - E_3) b_3 + \sum (\lambda E_r - E_r) b_r, \qquad 4 \leqq r \leqq n. \end{aligned}$$

Nach Satz 27 haben wir daher $G \supset \Omega(V, o(\rho)) \supset \Omega(V, (b_3))$, da $o(\rho) \supset (b_3)$. Damit ist (40) beweisen.

3. Jedenfalls ist $K \subset o(\sigma, B) \subset o(\sigma)$. Falls $K = L$, so folgt mit (40) auch (37). Wir nehmen daher an $K \subset I$. Wir betrachten jetzt alle Grössen modulo K und bezeichnen diese Äquivalenzklassen mit einem Querstrich. Wir behaupten

$$\Omega(\bar{V}, (\bar{u})) \subset \bar{G}. \tag{41}$$

Nach Folgerung (i) zu Theorem 4 (2. Teil) ist $\operatorname{Kern}(h_K : \Omega(V) \to \Omega(g_K V)) = \Omega(V, K)$. Daher können wir aus (41) und (40) auf (37) schiessen. Zum Beweis von (41) schreiben wir (38) und (39) modulo K auf:

$$\bar{\sigma}\bar{A} = \bar{A}\bar{a} + \bar{B}\bar{u}, \qquad \bar{\sigma}\bar{B} = \bar{A}\bar{v} + \bar{B}\bar{b}. \tag{42}$$

Auf Grund von (42) können wir $\bar{\sigma}$ in der Form

$$\bar{\sigma} = \bar{\kappa} \perp \bar{\mu}; \qquad \bar{\kappa} = \bar{\sigma} \mid P, \qquad \bar{\mu} = \bar{\sigma} \mid P^0 \tag{43}$$

schreiben. Für jedes $\bar{\lambda} \in \Omega(P^0)$ berachten wir das Element

$$\bar{\mu}(\bar{\lambda}) = \bar{\lambda}\bar{\mu}\bar{\lambda}^{-1}\bar{\mu}^{-1} \in \Omega(P^0) \cap \bar{G}.$$

Wir setzen $\bar{\mu}(\bar{\lambda})$ durch die Identität auf P fort und bezeichnen das so erklärte Element von $\Omega(\bar{V}) \cap \bar{G}$ wieder mit $\bar{\mu}(\bar{\lambda})$. Es ist $\bar{\mu}(\bar{\lambda}) \mid P = 1$. Nach Satz 27 folgt daraus

$$\Omega(\bar{V}, o(\bar{\mu}(\bar{\lambda}))) \subset \bar{G}. \tag{44}$$

4. Sei $\bar{J}$ das von den $o(\bar{\mu}(\bar{\lambda}))$ erzeugte Ideal. Aus (44) folgt

$$\Omega(\bar{V}, \bar{J}) \subset \bar{G}. \tag{45}$$

Wir behaupten

$$\bar{J} = o(\bar{\mu}). \tag{46}$$

Denn wegen $o(\bar{\mu}(\bar{\lambda})) \subset o(\bar{\mu})$ ist jedenfalls $\bar{J} \subset o(\bar{\mu})$ Angenommen, es wäre $\bar{J} \neq o(\bar{\mu})$. Dann ist also insbesondere $\bar{J} \subset \bar{I}$. Wir haben dann $h_{\bar{J}}\bar{\mu}(\bar{\lambda}) = h_{\bar{J}}\bar{\lambda} h_{\bar{J}}\bar{\mu} h_{\bar{J}}\bar{\lambda}^{-1} h_{\bar{J}}\bar{\mu}^{-1} = 1$ für alle $h_{\bar{J}}\bar{\lambda}$ von $h_{\bar{J}}\Omega(\bar{P}^0) = \Omega(g_{\bar{J}}P^0)$. Das heisst, $h_{\bar{J}}\bar{\mu}$ gehört zum Zentralisator von $\Omega(g_{\bar{J}}P^0)$, und daher, nach Satz 15, $h_{\bar{J}}\bar{\mu} = \pm 1$, also $o(\bar{\mu}) \subset \bar{J}$. Damit ist (46) bewiesen.

5. Mit (45) und (46) haben wir

$$\Omega(\bar{V}, o(\bar{\mu})) \subset \bar{G}. \tag{47}$$

Wenn $o(\bar{\mu}) = \bar{L}$, so gilt (41). Wir nehmen daher an $o(\bar{\mu}) \subset \bar{I}$. Wir betrachten jetzt alle quergestrichenen Grössen modulo $\bar{J} = o(\bar{\mu}) \subset \bar{I}$ und bezeichnen diese Äquivalenzklassen mit einem doppelten Querstrich. Aus (42) wird

$$\bar{\bar{\sigma}}\bar{\bar{A}} = \bar{\bar{A}}\bar{\bar{a}} + \bar{\bar{B}}\bar{\bar{u}}, \qquad \bar{\bar{\sigma}}\bar{\bar{B}} = \bar{\bar{A}}\bar{\bar{v}} + \bar{\bar{B}}\bar{\bar{b}}. \tag{48}$$

Da andererseits $\bar{\bar{\sigma}} \mid \bar{\bar{P}}^0 = 1$, folgt mit Satz 27, wegen $(\bar{\bar{u}}) \subset o(\bar{\bar{\sigma}})$

$$\Omega(\bar{\bar{V}}, (\bar{\bar{u}})) \subset \bar{\bar{G}}. \tag{49}$$

Da $\operatorname{Kern}(h_{\bar{J}}\colon \Omega(\bar{V}) \to \Omega(g_{\bar{J}}\bar{V})) = \Omega(\bar{V}, \bar{J})$, können wir aus (49) und (47) und (46) auf (41) und damit, wegen (40), auf (37) schliessen.

5.4. *Der Struktursatz : Theorem 6.*

THEOREM 6. *Sei* $\operatorname{ind} V \geqq 1$. *Sei* $\dim V \geqq 5$ *oder sei* $\dim V = 4$ *und* $\operatorname{ind} g_I V = 1$ *oder sei* $\dim V = 3$ *und* $L/I \neq \boldsymbol{F}_3$.

(i) *Jede Untergruppe G von $\boldsymbol{SO}(V)$ der Ordnung $o(G) = J$, die invariant ist unter $\Omega(V)$, genügt den Beziehungen*

$$\Omega(V, J) \subset G \subset \boldsymbol{SO}(V, J). \tag{50}$$

Andererseits ist eine Untergruppe G von $\boldsymbol{SO}(V)$, die den Beziehungen (50) *genügt, invariant und von der Ordnung J.*

(ii) *Eine invariante Untergruppe der Ordnung J von $\Omega(V)$ ist von der Form $\boldsymbol{SO}(V, J) \cap \Omega(V)$ oder $\Omega(V, J)$.*

Beweis. 1. Nach Folgerung 2 zu Theorem 3 ist $\Omega(V, J)$ invariant in $\boldsymbol{SO}(V)$ und von der Ordnung J. Nach Theorem 4(ii) ist $\boldsymbol{SO}(V, J)/\Omega(V, J)$ kommutativ. Also ist jede Untergruppe G von $\boldsymbol{SO}(V)$, die den Beziehungen (50) genügt, invariant in $\boldsymbol{SO}(V)$ und von der Ordnung J. (ii) ist eine unmittelbare Folge von (i) und Theorem 4(iii). Es bleibt also noch zu zeigen, dass jede unter $\Omega(V)$ invariante Untergruppe G von $\boldsymbol{SO}(V)$ der Ordnung J die Gruppe $\Omega(V, J)$ enthält. Wir unterscheiden drie Fälle.

2. Sei $\dim V = 3$. Dann ist $\operatorname{ind} V = 1$ und $L/I \neq \boldsymbol{F}_3$. Nach Theorem 5(ii) und der Ergänzung ist $\boldsymbol{SO}(V)$ isomorph zu $PGL(2, L)$ so, dass dabei

$\Omega(V)$ übergeht in $PSL(2,L)$ und G übergeht in eine unter $PSL(2,L)$ invariante Untergruppe G' von $PGL(2,L)$ der Ordnung J. Nach dem Struktursatz von $PGL(2,L)$, siehe Anhang, enthält G' daher die Gruppe $PSC(2,L,J)$, die der Gruppe $\Omega(V,J)$ entspricht, also $\Omega(V,J) \subset G$.

3. Sei $\dim V = 4$. Dann ist $\operatorname{ind} V = \operatorname{ind} g_I V = 1$. Nach Theorem 5(iii) und der Ergänzung ist $PS\boldsymbol{O}(V) = S\boldsymbol{O}(V)/\{1,-1\}$ isomorph einer Untergruppe $PU(2,L')$ von $PGL(2,L')$ so, dass dabei $P\Omega(V)$ übergeht in $PSL(2,L')$ und $PG = G/(G \cap \{1,-1\})$ übergeht in eine unter $PSL(2,L')$ invariante Untergruppe G' von $PU(2,L') \subset PGL(2,L')$ der Ordnung $J' = JL'$. Nach dem Struktursatz von $PGL(2,L')$, siehe Anhang, ist dann $PSC(2,L',J') \subset G'$, und da $PSC(2,L',J')$ der Gruppe

$$P\Omega(V,J) = \Omega(V,J)/(\Omega(V,J) \cap \{1,-1\}) = \Omega(V,J)/\{1\}$$

entspricht, ist $P\Omega(V,J) \subset PG$, also $\Omega(V,J) \subset G$.

4. Sei $\dim V \geqq 5$. Dann ist $\operatorname{ind} V \geqq 1$. $o(G) = J$ wird erzeugt von den Idealen $o(\sigma)$, wo σ die Elemente von G durchläuft. Nach Satz 28 ist $\Omega(V, o(\sigma)) \subset G$ für jedes $\sigma \in G$, also auch $\Omega(V,J) \subset G$.

Anhang: Die projektive lineare Gruppe in 2 Variablen.

Sei L ein lokaler Ring mit grösstem Ideal $I \neq L$ und sei $\operatorname{char} L/I \neq 2$. Mit $GL(2,L)$ und $SL(2,L)$ bezeichnen wir die *allgemeine* bzw. *spezielle lineare Gruppe in 2 Variablen über L*. In [5] hatten wir die Struktur dieser Gruppen bestimmt.

Für jedes Ideal J von L haben wir den kanonischen Homomorphismus

$$h_J\colon GL(2,L) \to GL(2,L/J). \tag{51}$$

Hier ist auch $J = L$ zugelassen; in diesem Falle soll $GL(2,L/J)$ die Einheitsgruppe E sein. Mit Hilfe von h_J, (51), und der Determinante, $\det\colon GL(2,L) \to L^*$, haben wir, für jedes Ideal J von L, folgende beiden invarianten Untergruppen von $GL(2,L)$, vgl. [5]:

$$GC(2,L,J) = \textit{Gruppe der } \sigma \in GL(2,L) \textit{ mit } h_J\sigma \in \text{Zentrum } GL(2,L/J),$$
$$SC(2,L,J) = \textit{Gruppe der } \sigma \in GL(2,L) \textit{ mit } h_J\sigma = 1 \textit{ und } \det\sigma = 1.$$

Das Zentrum von $GL(2,L/J)$ besteht, für $J \subset I$, aus den Homothetien, ist also isomorph zu $(L/J)^*$. Dagegen Zentrum $GL(2,L/L) = E$. Daher $GC(2,L,L) = GL(2,L)$, $GC(2,L,0) =$ Zentrum $GL(2,L)$, $SC(2,L,L) = SL(2,L)$.

Wir betrachten den kanonischen Homomorphismus

$$P\colon GL(2,L) \to GL(2,L)/\text{Zentrum } GL(2,L). \tag{52}$$

Das Bild $PGL(2, L)$ von $GL(2, L)$ unter P, (52), heisst *projektive lineare Gruppe in 2 Variablen über L.*

Der Homomorphismus h_J, (51), induziert einen Homomorphismus von $PGL(2, L)$ auf $PGL(2, L/J)$, den wir wieder mit h_J bezeichnen. Die Determinante induziert einem Homomorphismus, $PGL(2, L) \to L^*/L^{*2}$, für den wir wiederum det schreiben. Damit können wir die Bilder $PGC(2, L, J)$ und $PGC(2, L, J)$ der Gruppen $GC(2, L, J)$ und $SC(2, L, J)$ unter der Abbildung P, (52), folgendermassen charakterisieren:

$$PGC(2, L, J) = \textit{Gruppe der } \sigma \in PGL(2, L) \textit{ mit } h_J\sigma = 1 \in PGL(2, L/J),$$
$$PSC(2, L, J) = \textit{Gruppe der } \sigma \in PGL(2, L) \textit{ mit } h_J\sigma = 1 \textit{ und } \det \sigma = L^{*2}.$$

Die *Ordnung* $o(G)$ einer Untergruppe G von $GL(2, L)$ ist das kleinste Ideal J so, dass $G \subset GC(2, L, J)$. In [5] hatten wir gezeigt:

Sei $L/I \neq \mathbf{F}_3$. *Eine unter* $SL(2, L)$ *invariante Untergruppe* G *der Ordnung* $o(G) = J$ *genügt den Beziehungen* $SC(2, L, J) \subset G \subset GC(2, L, J)$. *Andererseits ist jede Untergruppe* G *von* $GL(2, L)$, *die diesen Beziehungen genügt, invariant in* $GL(2, L)$ *und von der Ordnung* J.

Unter der *Ordnung* $o(G')$ einer Untergruppe G' von $PGL(2, L)$ verstehen wir das kleinste Ideal J so, dass $G' \subset PGC(2, L, J)$. Wenn G eine Untergruppe von $GL(2, L)$ ist mit $PG = G'$, dann ist $o(G') = o(G)$. Das oben zitierte Ergebnis aus [5] liefert daher das folgende

STRUKTURTHEOREM FÜR $PGL(2, L)$. *Sei* L *ein lokaler Ring mit grössten Ideal* $I \neq L$ *und sei* $\operatorname{char} L/I \neq 2$ *und* $L/I \neq \mathbf{F}_3$. *Eine Untergruppe* G' *von* $PGL(2, L)$ *der Ordnung* $o(G') = J$, *die invariant ist unter* $PSL(2, L)$, *genügt den Beziehungen* $PSC(2, L, J) \subset G' \subset PGC(2, L, J)$. *Andererseits ist jede Untergruppe* G', *die diesen Beziehungen genügt, invariant in* $PGL(2, L)$ *und von der Ordnung* J.

UNIVERSITÄT GÖTTINGEN, GERMANY.

LITERATURVERZEICHNIS.

[1] E. Artin, *Geometric Algebra*, New York, 1957.
[2] N. Bourbaki, *Algèbre*, chap. 9, Paris, 1959.
[3] J. Dieudonné, *Sur les groupes classiques*, Paris, 1948.
[4] ———, *La géométrie des groupes classiques*, Berlin, 1955.
[5] W. Klingenberg, "Linear groups over local rings," *Bulletin of the American Mathematical Society*, vol. 66 (1960), pp. 294-296; "Lineare Gruppen über lokalen Ringen," *American Journal of Mathematics*, vol. 83 (1961), pp. 137-153.

SUR LES REPRÉSENTATIONS DES GROUPES CLASSIQUES 𝔭-ADIQUES I.*

par FRANÇOIS BRUHAT.

Soient G un groupe de Lie semi-simple réel linéaire et K un sous-groupe compact maximal de G: on sait depuis les travaux de Gelfand-Naimark, Harish-Chandra et R. Godement qu'une représentation irréductible de K intervient un nombre de fois inférieur à sa dimension dans la restriction à K de toute représentation complèment irréductible de G. De ce résultat, découle la théorie des "fonctions sphériques" sur G [4].

Il est naturel de chercher à étendre ce résultat aux groupes semi-simples sur un corps 𝔭-adique. C'est ce que nous faisons dans cet article pour le groupe spécial linéaire $SL(n,P)$ et pour certaines représentations d'un sous-groupe compact maximal K. Nous retrouvons ainsi en particulier un résultat obtenu par F. I. Mautner dans le cas du groupe spécial linéaire à deux variables et de la représentation unité de K [7]. Le cas des autres groupes classiques (orthogonal, symplectique, etc.) sera traité dans un article ultérieur.

1. Rappels et notations. Rappelons tout d'abord quelques résultats de la théorie des fonctions sphériques [4]. Soient G un groupe localement compact et K un sous-groupe compact de G. Soit U une représentation continue de G dans un espace de Banach $\mathfrak{H}$ et soit M une classe de représentations irréducibles de K. Soit χ_M le caractère de M et posons $r_M = \dim M$. Désignons par dx une mesure de Haar à droite sur G et par dk la mesure de Haar de masse totale 1 sur K. On sait que l'operateur

$$E(M) = r_M \int_K \bar{\chi}_M(k)\, U_k\, dk$$

est un projecteur continu sur le sous-espace $\mathfrak{H}(M)$ des éléments a de $\mathfrak{H}$ qui se transforment suivant M par la restriction de U à K (c'est-à-dire tels que le sous-espace F engendré par les $U_k a$ pour $k \in K$ soit de dimension finie et que la représentation de K dans F se décompose en somme de représentations irréductibles de classe M). Nous poserons $d_M(U) = \dim \mathfrak{H}(M)$.

Soit $\mathcal{L}(G)$ l'algèbre (pour la convolution) des fonctions continues à

---

* Received December 9, 1960.

support compact sur G et soit $\mathcal{L}(M)$ le sous-espace de $\mathcal{L}(G)$ formé des fonctions qui se transforment suivant M (resp. suivant la représentation $\bar{M}$ conjuguée de M) par la restriction à K de la représentation régulière gauche (resp. droite) de G. On voit aussitôt que les fonctions $f \in \mathcal{L}(M)$ sont les $f \in \mathcal{L}(G)$ satisfaisant aux relations:

$$f = (r_M \bar{\chi}_M) * f = f * (r_M \bar{\chi}_M).$$

On en déduit que $\mathcal{L}(M)$ est une *sous-algèbre* de $\mathcal{L}(G)$. Les relations d'orthogonalité des caractères d'un groupe compact entrainent que, pour $f \in \mathcal{L}(M)$, l'opérateur $U_f = \int_G f(x) U_x \, dx$ annule les sous-espaces $\mathcal{H}(M')$ pour $M' \neq M$ et conserve le sous-espace $\mathcal{H}(M)$. L'application $f \to U_f$ peut donc être considérée comme une représentation de $\mathcal{L}(M)$ dans $\mathcal{H}(M)$, que nous noterons U^M.

Rappelons d'autre part qu'un système Ω de représentations d'une algèbre A est dit *complet* si pour tout élément $a \neq 0$ de A il existe une représentation $U \in \Omega$ telle que $U_a \neq 0$. Avec cette terminologie, le résultat fondamental suivant est dû à R. Godement [4] : *s'il existe un système Ω de représentations continues du groupe G dans des espaces de Banach tel que:*

a) *les représentations U^M pour $U \in \Omega$ forment un système complet de représentations de l'algèbre $\mathcal{L}(M)$;*

b) *il existe un entier $p \geqq 0$ tel que $d_M(U) \leqq p \dim M$ pour tout $U \in \Omega$; alors, on a $d_M(U) \leqq p \dim M$ pour toute représentation complétement irréductible U dans un espace de Banach* (on dit encore que *M est contenue au plus p fois dans toute représentation complétement irréductible de G*).

Durant tout ce travail, les notations suivantes seront utilisées:

P est un corps valué complet, non archimédien et localement compact;

v désigne la valuation (discrète) de P, supposée normée (c'est-à dire ayant le groupe des entiers comme groupe de valeurs);

$\mathcal{O}$ désigne l'anneau des entiers de P;

$\mathcal{O}^*$ désigne l'ensemble $\mathcal{O}$-$\mathfrak{p}$ des éléments inversibles de $\mathcal{O}$;

$\mathfrak{p}$ est l'idéal maximal de $\mathcal{O}$;

π est une uniformisante (c'est à dire un générateur de $\mathfrak{p}$), choisie une fois toutes;

F_q désigne le corps des restes $\mathcal{O}/\mathfrak{p}$ de P: c'est un corps fini à q éléments.

2. Quelques Lemmes sur $SL(n, P)$. Dans les n° 2 et 3, nous désignerons par G le groupe $SL(n, P)$ des matrices carrées de déterminant 1 à coefficients dans le corps localement compact P. Pour $g \in G$, nous désignerons par g_{ij} (pour $1 \leqq i, j \leqq n$) les éléments de la matrice g. Nous désignerons par:

Γ (resp. Γ') le sous-groupe de G formé des matrices triangulaires supérieures (resp. inférieures) : on a $g \in \Gamma$ si et seulement si $g_{ij} = 0$ pour $j < i$;

T (resp. T') le sous-groupe de Γ (resp. Γ') formé des matrices dont les coefficients diagonaux sont des puissances entières positives ou négatives de π;

N (resp. N') le sous-groupe de T (resp. T') formé des matrices unipotentes (de coefficients diagonaux égaux à 1);

D le sous-groupe $\Gamma \cap \Gamma'$ des matrices diagonales;

Δ le sous-groupe $T \cap D$ des matrices diagonales dont les coefficients diagonaux sont des puissances de π.

Soit A l'ensemble des systèmes $\alpha = (\alpha_1, \cdots, \alpha_n)$ de n entiers tels que $\sum \alpha_i = 0$ et A^+ l'ensemble des $\alpha \in A$ tels que $\alpha_1 \leqq \alpha_2 \leqq \cdots \leqq \alpha_n$. Pour tout $\alpha \in A$, nous désignerons par d_α l'élément de Δ défini par les relations $(d_\alpha)_{ii} = \pi^{\alpha_i}$. Nous noterons Δ^+ l'ensemble des d_α pour $\alpha \in A^+$.

On vérifie aussitot que N et T sont des sous-groupes distingués de Γ. De plus, on a $\Gamma = DN = ND$ et $T = \Delta N = N\Delta$ avec $D \cap N = \Delta \cap N = \{e\}$: autrement dit, Γ (resp. T) est produit semi-direct de N et de D (resp. Δ).

Enfin, nous désignerons par K le sous-groupe de G formé des éléments dont les coefficients sont *entiers*: autrement dit, on a $K = SL(n, \mathfrak{O})$. Comme $\mathfrak{O}$ est un sous-groupe ouvert et compact de P, on voit que K *est un sous-groupe ouvert et compact de* G. Par suite, une mesure de Haar sur G induit sur K une mesure de Haar et on peut ainsi normaliser la mesure de Haar dg sur G de telle sort que $\int_K dg = 1$.

Le résultat suivant est bien connu: on en trouvera d'ailleurs une démonstration valable pour tous les groupes simples de Chevalley sur un corps $\mathfrak{p}$-adique dans [3]. Pour être complet, nous allons en donner une démonstration élémentaire:

Lemme 1. *On a* $G = TK$.

Nous allons raisonner par récurrence sur n: l'assertion est évidente si $n = 1$. Supposons donc $n > 1$ et le Lemme démontré pour les groupes $SL(m, P)$ avec $m < n$. Il nous suffit de montrer que, pour tout $g \in G$, il existe un $k \in K$ et un $t \in T$ tels que $tgk \in T$. Le système d'équations linéaires homogènes

$$\sum_{j=1}^{j=n} g_{ij} x_j = 0 \qquad \text{pour } 1 < i \leqq n$$

a toujours une solution non nulle. Par multiplication par un élément convenable de P, on peut en déduire une solution (x_j) appartenant à $\mathcal{O}^n$ et telle qu'il existe un indice a avec $1 \leqq a \leqq n$ et $x_a = 1$. Désignons alors par δ_{ij} l'indice de Kronecker et posons:

$$\begin{array}{ll} k_{ij} = \delta_{ij} & \text{pour } 1 \leqq i < a \text{ et } j > 1, \\ k_{aj} = 0 & \text{pour } j > 1, \\ k_{ij} = \delta_{(i-1)j} & \text{pour } a < i \leqq n \text{ et } j > 1, \\ k_{i1} = (-1)^{a+1} x_i & \text{pour } 1 \leqq i \leqq n. \end{array}$$

On vérifie aussitot que la matrice $k = (k_{ij})_{1 \leqq i, j \leqq n}$ appartient à K et que l'élément $g' = gk$ est tel que $g'_{i1} = 0$ pour $1 < i \leqq n$. Par suite, on a $g_{11} \neq 0$ et il existe un entier α et un élément $y \in \mathcal{O}^*$ tels que $g'_{11} = \pi^{\alpha} y$. Soit alors $t \in \Delta$ tel que $t_{11} = \pi^{-\alpha}$ et soit $k' \in D \cap K$ tel que $k'_{11} = y^{-1}$: l'élément $g'' = tg'k' = tgkk'$ est alors tel que $g''_{i1} = 0$ pour $1 < i \leqq n$ et $g''_{11} = 1$. La matrice $g^0 = (g''_{ij})_{2 \leqq i, j \leqq n}$ est alors un élément de $SL(n-1, P)$ et d'après l'hypothèse de récurrence, il existe une matrice $h' = (h'_{ij})_{2 \leqq i, j \leqq n}$ de déterminant 1, à coefficients dans $\mathcal{O}$ telle que $g^0 h'$ soit une matrice triangulaire supérieure, dont les coefficients diagonaux sont des puissances de π.

Posons alors $h_{ij} = h'_{ij}$ pour $2 \leqq i, j \leqq n$, $h_{1i} = h_{i1} = 0$ pour $1 < i \leqq n$ et $h_{11} = 1$: nous obtenons un élément $h = (h_{ij})$ de K et on vérifie immédiatement que $g''h = tgkk'h$ appartient à T.

Remarque. Il est clair que la décomposition $g = tk$ n'est pas unique, contrairement à ce qui se passe, mutatis mutandis, dans le cas des groupes de Lie réels. Cependent comme $T \cap K = N \cap K$, les coefficients diagonaux de t sont bien déterminés: si on a $d' = ndk$ (avec $d, d' \in \Delta$, $n \in N$ et $k \in K$), on a $d^{-1}n^{-1}d' = d^{-1}n^{-1}d \cdot d^{-1}d' \in N$ d'où $d^{-1}d' \in N$ et $d = d'$.

Passons maintenant à l'étude des doubles classes modulo K:

LEMME 2. *Dans toute double classe modulo K il y a un élément de Δ^+ et un seul.*

C'est une conséquence immédiate du théorème des diviseurs élémentaires. Soit en effet $g \in G$; posons $\omega = \inf v(g_{ij})$: on a $\omega \leqq 0$ puisque $\det g = 1$. Posons $a_{ij} = \pi^{-\omega} g_{ij}$. La matrice $a = (a_{ij})$ est alors à coefficients entiers. Comme $\mathcal{O}$ est un anneau principal, le théorème des diviseurs élémentaires (cf. [1], § 4, prop. 4) entraine qu'il existe une matrice diagonale d' et une seule dont les coefficients diagonaux d'_{ii} soient des puissances entières π^{β_i} de l'uniformisante π et satisfaisant aux deux conditions:

1) $\beta_1 \leqq \beta_2 \leqq \cdots \leqq \beta_n$,

2) il existe deux éléments inversibles k_1 et k_2 de l'anneau des matrices d'ordre n à coefficients dans $\mathfrak{O}$ tels que $d' = k_1 a k_2$. (Nous avons utilisé le fait que un idéal quelconque de $\mathfrak{O}$ admet une puissance de π comme générateur). De plus, on sait ([1], § 4, prop. 3) que les entiers β_i sont déterminés comme suit: pour tout entier p avec $1 \leqq p \leqq n$, la somme $\sum_{i=1}^{i=p} \beta_i$ est égale à la borne inférieure des valuations des mineurs d'ordre p de la matrice a. En particulier, on a $\beta_i = 0$ et $\sum_{i=1}^{i=n} \beta_i = -n\omega$. On a donc dét $d' =$ dét a et par suite dét $k_1 = (\text{dét}\, k_2)^{-1}$. En multipliant la première ligne de k_1 par dét k_2 et la première colonne de k_2 par dét k_1, on voit qu'on peut supposer dans la condition 2) que dét $k_1 =$ dét $k_2 = 1$, autrement dit que k_1 et $k_2 \in K$.

Revenant à g, on en déduit aussitot le Lemme 2, avec de plus la précision suivante: pour que $g \in K d_\alpha K$ (avec $d_\alpha \in \Delta^+$), il faut et il suffit que, pour tout p avec $1 \leqq p \leqq n$, la somme $\sum_{i=1}^{i=p} \alpha_i$ soit égale à la borne inférieure des valuations des mineurs d'ordre p de g. En particulier, on a $\alpha_1 = \inf v(g_{ij})$.

Corollaire. *K est un sous-groupe compact maximal de G.*

En effet, si un sous-groupe A de G contient K et est $\neq K$, il contient un élément $d_\alpha \in \Delta$ avec $d_\alpha \neq 0$. Mais le sous-groupe engendré par un tel d_α n'est pas relativement compact, car les valuations des coefficients de ses éléments ne sont pas bornées inférieurement.

Remarquons qu'il est bien connu que réciproquement, tout sous-groupe compact de G est contenuu dans un transformé xKx^{-1} de K par un élément x du groupe linéaire $GL(n, P)$: c'est une conséquence facile du théorème des diviseurs élémentaires, que nous ne démontrerons pas, car nous n'en aurons pas besoin.

Etudions enfin les rapports entre les décompositions de G en doubles classes modulo K donnée par le Lemme 2 et en classes à gauche modulo K donnée par le Lemme 1. Tout d'abord, toute classe à gauche gK et toute double classe KgK sont ouvertes et compactes. Par suite une double classe est réunion d'un nombre fini de classes à gauche.

Ordonnons totalement A par l'ordre lexicographique: $\beta = (\beta_1, \cdots, \beta_n)$ est supérieur à $\alpha = (\alpha_1, \cdots, \alpha_n)$ si et seulement si l'on a $\beta_i > \alpha_i$ pour le plus petit indice i tel que $\beta_i \neq \alpha_i$.

Lemme 3. *Soit $\alpha \in A^+$. Si $N d_\beta K \cap K d_\alpha K$ n'est pas vide, alors $\beta \geqq \alpha$. De plus, on a $N d_\alpha K \cap K d_\alpha K = d_\alpha K$.*

Soit en effet $n \in N$ tel que $nd_\beta \in Kd_\alpha K$: cela signifie d'après ce qui précède, que la borne inférieure des valuations des mineurs d'ordre p de nd_β est, pour tout entier p avec $1 \leqq p \leqq n$, égale à $\sum_{i=1}^{i=p} \alpha_i$. En considérant le mineur formé des p premières lignes et colonnes de nd_β, on en déduit aussitôt que $\sum_{i=1}^{i=p} \beta_i \geqq \sum_{i=1}^{i=p} \alpha_i$ pour tout p, donc que $\beta \geqq \alpha$.

Soit maintenant $n \in N$ tel que $g = nd_\alpha \in Kd_\alpha K$. Considérons pour $1 \leqq i < j \leqq n$ le mineur A_{ij} d'ordre i de g obtenu en supprimant les $(n - i)$ dernières lignes et les $(n - i + 1)$ dernières colonnes excepté la colonne d'indice j. On a $A_{ij} = \pi^{\alpha_1 + \cdots + \alpha_{i-1}} g_{ij}$ et par suite, on a:

$$\sum_{r=1}^{r=i} \alpha_r \leqq v(A_{ij}) = \alpha_1 + \cdots + \alpha_{i-1} + v(g_{ij})$$

et par suite $u(g_{ij}) \geqq \alpha_i$.

On peut alors, par récurrence sur j, déterminer pour $1 \leqq i < j \leqq n$ des éléments $k_{ij} \in \mathfrak{O}$ tels que:

$$\sum_{r=i+1}^{r=j-1} g_{ir} k_{rj} + g_{ij} = -\pi^{\alpha_i} k_{ij} \tag{1}$$

le premier membre de (1) étant de valuation $\geqq \alpha_i$. Complétons alors ces k_{ij} en une matrice $k \in K \cap N$ en posant $k_{ii} = 1$ pour tout i et $k_{ij} = 0$ pour $i > j$: on vérifie aussitot que $gk = d_\alpha$ et par suite $g \in d_\alpha K$, d'où la seconde assertion du Lemme 3.

Pour tout $\alpha \in A^+$, nous désignerons par $I(\alpha)$ l'ensemble (fini) des classes à gauche modulo K contenues dans $Kd_\alpha K$. Dans chaque classe $c \in I(\alpha)$, choisissons un élément $t(c) \in c \cap T$ élément qui s'écrit d'une manière et d'une seule sous la forme $n(c) d_{\gamma(c)}$ avec $n(c) \in N$ et $\gamma(c) \in A$. Le Lemme 3 montre que $\gamma(c) \geqq \alpha$ pour tout $c \in I(\alpha)$ et qu'il existe un et un seul $c_\alpha \in I(\alpha)$ tel que $\gamma(c_\alpha) = \alpha$: nous prendrons toujours $t(c_\alpha) = d_\alpha$ (donc $n(c_\alpha) = e$).

3. Le résultat principal. Soit λ un caractère du groupe abélien discret Δ; comme Δ s'identifie au groupe quotient T/N, on peut considérer λ comme un caractère de T (et on obtient ainsi tous les caractères de T, car N est le groupe des commutateurs de T). Nous allons chercher à montrer que l'on obtient "beaucoup" de représentations de G en considérant les représentations unitaires de G induites par les divers caractères unitaires λ de T. Pour la définition et les propriétés élémentaires des représentations induites, nous renvoyons à [2] et à [6].

Désignons par ρ une "fonction ρ" sur G relative à T au sens de [2] (p. 102), c'est à dire une fonction continue strictement positive sur G, avec $\rho(e) = 1$ et $\rho(tx) = (\delta_T(t)/\delta_G(t))\rho(x)$ pour tout $x \in G$ et tout $t \in T$ (où δ_T (resp. δ_G) désigne le module de T (resp. G)). La restriction de ρ à T est un caractère réel positif de T. On a donc $\rho = 1$ sur tout sous-groupe compact de T, en particulier sur $T \cap K$. On montre aisément (en utilisant le lemme 1 et le fait que K est ouvert et compact) que l'espace $\mathcal{H}^\lambda$ de la représentation U^λ de G induite par le caractère unitaire λ de T est l'espace des fonctions ϕ sur G satisfaisant aux deux conditions:

(2) $\phi(tx) = \rho(t)^{-\frac{1}{2}}\lambda(t)\phi(x)$ pour tout $x \in G$ et tout $t \in T$,

(3) la restriction ϕ^0 de ϕ au sous-groupe K est de carré intégrable, et G opère dans $\mathcal{H}^\lambda$ par translation à droite. De plus, l'application $\phi \rightarrow \phi^0$ est un isomorphisme de l'espace de Hilbert $\mathcal{H}^\lambda$ sur le sous-espace fermé $\mathcal{H}$ de $L^2(K)$ formé des fonctions ϕ satisfaisant à la condition (2) pour tout $x \in K$ et tout $t \in T \cap K$. Mais on a $\rho(t) = 1$ sur $T \cap K$ et d'autre part, on a $T \cap K = N \cap K$ et par suite on a aussi $\lambda(t) = 1$ pour $t \in T \cap K$. L'espace $\mathcal{H}$ est donc simplement le sous-espace fermé de $L^2(K)$ formé des fonctions invariantes par les translations à gauche par les éléments de $N \cap K$ et est en particulier indépendant de λ (mais naturellement, la représentation de G dans $\mathcal{H}$ déduite de U^λ dépend elle de λ).

Remarque 1. Comme D est produit direct de Δ et de $D \cap K$, la représentation ${}^DU^\lambda$ de D induite par le caractère λ de Δ est le produit du caractère λ par la représentation régulière de $D \cap K$. Comme $D \cap K$ est compact, ${}^DU^\lambda$ se décompose en la somme directe discrète des caractères unitaires de D égaux à λ sur Δ. On en déduit que la représentation de Γ induite par le caractère λ de T se décompose en somme directe discrète de caractères de Γ. Le théorème d'induction par étages montre alors que la représentation U^λ de G se décompose en somme directe discrète des représentations de G induites par les caractères de Γ égaux à λ sur T (représentations de la "série principale," qui sont "en général" irréductibles ([3], théorème 6)). Par suite, on obtient les mêmes résultats au point de vue qui nous intéresse (savoir dans quelle mesure le système des U^λ est complet) en considérant les représentations induites par les caractères unitaires de T ou ceux de Γ.

Remarque 2. Dans le cas des groupes unimodulaires réels ou complexes, les représentations induites par les caractères unitaires de T forment un système *complet* de représentations de G [4]. Ici, au contraire, ces représentations *ne forment pas* un système complet (même si l'on prend tous les caractères de Δ, non nécessairement unitaires). En effet, l'algèbre $\mathscr{L}(K)$ est une sous-algèbre de $\mathscr{L}(G)$ (puisque K est ouvert dans G). Si les U^λ formaient un système complet, leurs restrictions à K formeraient un système complet de représentations de K. Les relations d'orthogonalité sur un groupe compact entrainent qu'une représentation irréductible quelconque de K serait contenue dans l'une au moins des U^λ. Or la restriction de U^λ à K est la représentation de K induite par le caractère unité de $N \cap K$ et le théorème de réciprocité de Frobenius montre que les représentations irréductibles qui interviennent dans la restriction de U^λ à K sont exactement celles dont la restriction à $N \cap K$ contient la représentation unité. Or il existe des représentations irréductibles de K, provenant par exemple de représentations du groupe fini $SL(n, F_q)$ (qui est un quotient de K), qui ne possèdent pas cette propriété [8]. On voit par suite que l'utilisation des U^λ ne nous permettra d'obtenir de renseignements que pour les "fonctions sphériques" correspondant à certaines représentations de K, celles dont la restriction à $N \cap K$ contient la représentation unité.

Soit $f \in \mathscr{L}(G)$ avec $f \neq 0$. Nous cherchons à démontrer qu'il existe un caractère λ de Δ tel que $U^\lambda{}_f \neq 0$. Nous allons donc supposer que $U^\lambda{}_f = 0$ pour tout λ et étudier les conséquences de cette hypothèse. Soit Σ le support (compact) de f: il ne rencontre qu'un nombre fini de doubles classes modulo K. Nous désignerons par $S(f)$ (ou plus simplement par S) l'ensemble (fini non vide) des $\beta \in A^+$ tels que Σ rencontre $Kd_\beta K$ et par $\alpha(f)$ (ou plus simplement α) le plus petit élément de $S(f)$. Pour $\phi \in \mathscr{H}^\lambda$, et ϕ continue, nous avons (en désignant par e l'élément neutre de G):

$$\begin{aligned}(U^\lambda{}_f \cdot \phi)(e) &= \int_G \phi(x) f(x)\,dx \\ &= \sum_{\beta \in S} \sum_{c \in I(\beta)} \int_K \phi(n(c) d_{\gamma(c)} k) f(n(c) d_{\gamma(c)} k)\,dk \\ &= \sum_{\beta \in S} \sum_{c \in I(\beta)} \rho(t(c))^{-\frac{1}{2}} \lambda(d_{\gamma(c)}) \int_K \phi^0(k) f(t(c)k)\,dk\end{aligned}$$

et les indices $\gamma(c)$ sont (pour $\beta \in S$ et $c \in I(\beta)$) tous supérieurs à α. De plus, l'indice α n'intervient qu'*une seule fois* dans la sommation, pour $\beta = \alpha$ et $c = c_\alpha$. Nous avons donc obtenu une relation de la forme:

$$(4) \qquad (U^\lambda{}_f \cdot \phi)(e) = \sum_{\gamma \geqq \alpha} Q_\gamma(\phi^0) \lambda(d_\gamma)$$

avec:

$$(5) \qquad Q_\gamma(\phi^0) = \sum_{\beta \in S,\, c \in I(\beta),\, \gamma(c) = \gamma} \rho(t(c))^{-\frac{1}{2}} \int_K \phi^0(k) f(t(c)k)\,dk$$

et en particulier:

$$Q_\alpha(\phi^0) = \rho(d_\alpha)^{-\frac{1}{2}} \int_K \phi^0(k) f(d_\alpha k)\, dk. \tag{6}$$

Or, pour tout $\gamma \in A$, l'application $\lambda \to \lambda(d_\gamma)$ est un caractère unitaire γ^* du groupe dual Δ^* de Δ et à deux γ distincts correspondre deux caractères γ^* distincts. Les caractères d'un groupe étant linéairement indépendants, la relation $\sum Q_\gamma(\phi^0)\lambda(d_\gamma) = 0$ pour tout $\lambda \in \Delta^*$ entraine donc $Q_\gamma(\phi^0) = 0$ pour tout γ et en particulier $Q_\alpha(\phi^0) = 0$.

Par suite, si $U^\lambda{}_f = 0$ pour tout λ, alors on a

$$\int_K \phi(k) f(d_\alpha k)\, dk = 0 \text{ pour toute } \phi \in \mathfrak{H}.$$

Mais, pour tous $h, h' \in K$, la condition $U^\lambda{}_f = 0$ est équivalente à $U^\lambda{}_g = 0$ où g est la fonction $x \to f(h^{-1}xh')$, puisque l'on a $U^\lambda{}_g = U^\lambda{}_h U^\lambda{}_f U^\lambda{}_{h'}$. De plus, on a $S(f) = S(g)$ et $\alpha(f) = \alpha(g)$. Par suite, si $U^\lambda{}_f = 0$ pour tout λ, nous avons aussi:

$$\int_K \phi(k) f(k_1 d_\alpha k k_2)\, dk = 0 \tag{7}$$

pour toute $\phi \in \mathfrak{H}$ et tous $k_1, k_2 \in K$.

Posons alors $K_\alpha = K \cap d_\alpha^{-1} K d_\alpha$. Soit $h_1 \in K_\alpha$ et $h_2 \in K$; prenons $k_1 = d_\alpha h_1^{-1} d_\alpha^{-1}$ et $k_2 = h_2^{-1}$ dans (7): nous obtenons:

$$\int_K \phi(h_1 k h_2) f(d_\alpha k)\, dk = \int_K \phi(k) f(k_1 d_\alpha k k_2)\, dk = 0 \tag{8}$$

d'où le résultat suivant:

LEMME 4. *Soit* $f \in \mathcal{L}(G)$ *avec* $f \neq 0$. *Posons* $\alpha = \alpha(f)$ *et supposons que* $U^\lambda{}_f = 0$ *pour tout* $\lambda \in \Delta^*$. *Alors la fonction* $k \to f(d_\alpha k)$ *est orthogonale dans* $\mathcal{L}^2(K)$ *à toutes les translatées à gauche par des éléments de* K_α *et à droite par des éléments de* K *des fonctions appartenant à* $\mathfrak{H}$.

Remarquons que $\mathfrak{H}$ est invariant par les translations à droite par les éléments de K et qu'on pourrait donc sans rien perdre supprimer les translations à droite dans l'énoncé du Lemme 4.

Etudions maintenant le sous-groupe K_α:

LEMME 5. *Pour tout* $\alpha \in A^+$, *le sous-groupe* K_α *contient le sous-groupe* $K \cap \Gamma'$ *de* K.

En effet si $k = (k_{ij}) \in K$, on a $(d_\alpha^{-1} k d_\alpha)_{ij} = \pi^{\alpha_j - \alpha_i} k_{ij}$. Par suite, le sous-groupe K^α est formé des matrices $k \in K$ telles que $\pi^{\alpha_i - \alpha_j} k_{ij}$ soit entier quels que soient i et j. Or si $k \in K \cap \Gamma'$, on a $k_{ij} = 0$ pour $i < j$ et $\pi^{\alpha_i - \alpha_j} k_{ij} \in \mathfrak{O}$ pour $i \geqq j$, puisque $\alpha_i \geqq \alpha_j$ pour $i \geqq j$.

Nous allons maintenant considérer une représentation irréductible de K dans un espace de dimension finie E satisfaisant à la condition suivante:

(S) *les transformés par les opérateurs M_x pour $x \in K \cap \Gamma'$ des éléments de E invariants par les opérateurs M_y pour $y \in K \cap N$ forment un ensemble total dans E.*

Remarquons que, comme $\Gamma' = N'D$ et que N est un sous-groupe distingué de $\Gamma = ND$, le transformé par un opérateur M_x pour $x \in K \cap D$ d'un élément de E invariant par $K \cap N$. Par suite, on peut dans la condition (S) remplacer le sous-groupe $K \cap \Gamma'$ par le sous-groupe $K \cap N'$.

Nous pouvons maintenant démontrer notre principal résultat: avec les notations du n° 1, on a le:

Théorème 1. *Soit M une représentation irréductible de K satisfaisant à la condition* (S). *Les représentations $(U^\lambda)^M$ pour $\lambda \in \Delta^*$, forment un système complet de représentations de l'algèbre $\mathcal{L}(M)$.*

Nous pouvons supposer que M est réalisée comme sous-représentation irréductible de la représentation régulière *gauche* dans un sous-espace E de $L^2(K)$. Soit $f \in \mathcal{L}(M)$, $f \neq 0$ et supposons que $U^\lambda{}_f = 0$ pour tout λ. Pour tout $h \in K$, la fonction $g \colon x \rightarrow f(hx)$ appartient encore à $\mathcal{L}(M)$ et $U^\lambda{}_f = 0$ est équivalent à $U^\lambda{}_g = 0$. Nous pouvons donc, quitte à remplacer f par g pour un choix convenable de h, supposer que la fonction $\phi(k) = f(d_\alpha k)$ (avec $\alpha = \alpha(f) = \alpha(g)$) n'est pas nulle sur K.

Soit F le sous-espace de $L^2(K)$ formé de éléments qui se transforment suivant la représentation conjuguée $\bar{M}$ de M par la représentation régulière *droite* de K: on sait que c'est aussi l'ensemble des éléments qui se transforment suivant M par la représentation régulière *gauche* de K. On a donc $E \subset F$. De plus, la double représentation régulière de K restreinte à F est irréductible. Par suite, les translatés à droite des éléments de E forment un ensemble total dans F. La condition (S) et le Lemme 5 entrainent donc que les translatés à droite par K des translatés à gauche par K_α des éléments de E invariants par $N \cap K$ (c'est à dire des éléments de $E \cap \mathfrak{H}$) forment, pour tout $\alpha \in A^+$, un ensemble total dans F.

Par suite, d'après le Lemme 4, la fonction $\phi(k)$ est orthogonale à F. Mais puisque $f \in \mathcal{L}(M)$, la fonction f, donc aussi la fonction $\phi(k) = f(d_\alpha k)$, se transforme suivant $\bar{M}$ par la représentation régulière droite de G restreinte à K. Autrement dit, ϕ est un élément non nul de F, d'où une contradiction: par suite, les conditions $f \in \mathcal{L}(M)$ et $U^{\lambda}{}_{f} = 0$ pour tout λ entrainent $f = 0$, d'où le théorème.

COROLLAIRE 1. *Soit M une classe de représentations irréductibles de K satisfaisant à la condition* (S). *Alors M est contenue au plus* $\dim M$ *fois dans toute représentation complètement irréductible de G.*

Il suffit d'après le résultat fondamental de R. Godement rappelé au n° 1, de montrer que $\dim \mathcal{H}^{\lambda}(M) \leqq (\dim M)^2$ pour tout λ, ce qui est évident puisque U^{λ} restreinte à K s'identifie à une sous-représentation de la représentation régulière gauche de K.

COROLLAIRE 2. *La représentation unité de K est contenue au plus une fois dans toute représentation complètement irréductible de G.*

En effet, il est clair que la représentation unité satifait à la condition (S).

COROLLAIRE 3. *Si M est la représentation unité, l'algèbre $\mathcal{L}(M)$ est commutative.*

En effet, l'algèbre $\mathcal{L}(M)$ admet alors un système complet de représentations de dimension 1.

Les Corollaires 2 et 3 redonnent, dans le cas $n = 2$, des résultats dus à F. I. Mautner [7].

4. Exemple de représentations satisfaisant à (S). Le groupe $SL(n, F_q)$ des matrices de déterminant à coefficients dans le corps des restes F_q du corps $\mathfrak{p}$-adique P est canoniquement isomorphe au goupe quotient de $K = SL(n, \mathfrak{O})$ par le sous-groupe invariant des matrices entières congrues à l'unité modulo $\mathfrak{p}$. Par suite, une représentation de $SL(n, F_q)$ détermine canoniquement une représentation de K: nous dirons que cette dernière "provient" d'une représentation de $SL(n, F_q)$. Nous allons démontrer le résultat suivant:

THÉORÈME 2. *Toute représentation irréductible M de $K = SL(n, \mathfrak{O})$ qui provient d'une représentation de $SL(n, F_q)$ et dont la restriction à $N \cap K$ contient la représentation unité, satisfait à la condition* (S).

Changeons de notations: dans le reste de ce n°, G désignera le groupe $SL(n, F_q)$, Γ (resp. Γ') le sous-groupe des matrices triangulaires supérieures (resp. inférieures) de G, N (resp. N') le sous-groupe des matrices unipotentes de Γ (resp. Γ'). Soit $\mathfrak{R}$ l'ensemble des représentations irréductibles de G

dont la restriction à N contient la représentation unité. Il est clair que le Théorème 2 est équivalent à l'assertion suivante: toute représentation $M \in \mathfrak{R}$ satisfait à la condition:

(S′) les transformés par les opérateurs M_x pour $x \in N'$ des éléments invariants par les opérateurs M_y pour $y \in N$, forment un ensemble total dans l'espace de M.

Le théorème de Frobenius montre que les représentations $M \in \mathfrak{R}$ sont exactement les composantes irréductibles de la représentation de G induite par le caractère unité de N. Or cette dernière représentation se décompose en la somme directe des représentations de G induites par les caractères de Γ (cf. n° 3, Remarque 1). D'autre part, on vérifie facilement que pour qu'une représentation de G satisfasse à (S′), il faut et il suffit que toutes ses composantes irréductibles y satisfassent. Le Théorème 2 sera donc conséquence du:

LEMME 6. *Soit* λ *un caractère de* Γ *et soit* $\mathfrak{H}^0$ *le sous-espace de* $\mathfrak{H}^\lambda$ *engendré par les transformés par* N' *des éléments de* $\mathfrak{H}^\lambda$ *invariants par* N. *On a* $\mathfrak{H}^0 = \mathfrak{H}^\lambda$.

Le reste de ce n° est consacré à la démonstration du Lemme 6. Etudions la restriction de U^λ à N. Pour toute classe à droite $D = \Gamma x$, désignons par f_D un élément $\neq 0$ de $\mathfrak{H}^\lambda$ nul en dehors de D: il est clair que f_D est déterminé à une constante multiplicative près et que les f_D forment, quand D décrit G/Γ, une *base* de $\mathfrak{H}^\lambda$. De plus, les opérations de G dans $\mathfrak{H}^\lambda$ permutent entre elles, à des scalaires multiplicatifs près, les différents f_D. Soit maintenant $C = \Gamma x N$ une double classe modulo $(\Gamma : N)$ et soit $\mathfrak{H}_C$ le sous-espace de $\mathfrak{H}^\lambda$ formé des fonctions nulles en dehors de C. Il est clair que $\mathfrak{H}_C$ est invariant par N et la représentation de N dans $\mathfrak{H}_C$ est équivalente à la représentation de N induite par le caractère $\lambda_x : n \rightarrow \lambda(xnx^{-1})$ du sous-groupe $N \cap x^{-1}\Gamma x$ de N ([5], th. 1). Mais, si $n \in N \cap x^{-1}\Gamma x$, alors xnx^{-1} est une matrice unipotente de Γ, donc appartient à N, et on a $\lambda(xnx^{-1}) = 1$, puisque N est le groupe des commutateurs de Γ. Par suite, λ_x est le caractère unité et le théorème de Frobenius entraine que la représentation de N dans $\mathfrak{H}_C$ contient la représentation unité. D'où:

LEMME 7. *Pour toute classe à droite* D_1 *modulo* Γ, *il existe dans* $\mathfrak{H}^0$ *un élément* $\phi(D_1) \neq 0$ *invariant par* N *et de la forme* $\sum a(D) f_D$, *la somme étant étendue aux classes à droite* D *modulo* Γ *qui sont contenues dans la double classe* $D_1 N$. *On a* $a(D_1) \neq 0$.

En effet, comme N est transitif sur l'ensemble des classes à droite D contenues dans $D_1 N$, si l'on avait $a(D_1) = 0$, l'on aurait aussi $\phi(D_1) = 0$.

Nous allons maintenant interpréter géométriquement classes à droite modulo Γ et doubles classes modulo $(\Gamma: N)$. Soit S un espace vectoriel de dimension n sur F_q. Rappelons qu'un *drapeau* de type $(\alpha_1, \cdots, \alpha_k)$ de S (où les α_i sont des entiers positifs avec $0 \leqq \alpha_1 \leqq \alpha_2 \leqq \cdots \leqq \alpha_k \leqq n$) est l'ensemble de k sous-espaces vectoriels $D^1, \cdots, D^k$ de S avec $D^1 \subset D^2 \subset \cdots \subset D^k$ et $\dim D^i = \alpha_i$. Nous appelerons *drapeau complet* un drapeau de type $(1, 2, \cdots, (n-1))$.

Soient $D_0 = (D_0^1, \cdots, D_0^{n-1})$ et $D_\infty = (D_\infty^1, \cdots, D_\infty^{n-1})$ deux drapeaux complets en "position générale," c'est à dire tels que l'espace S soit, pour tout j, somme directe de D_0^j et de D_∞^{n-j}, ou encore que les dimensions des intersections $D_0^i \cap D_\infty^j$ soient, pour tous i, j, les plus petites possibles, compte tenu des dimensions de D_0^i et de D_∞^j. Pour $1 \leqq j \leqq n$, l'intersection $D_0^j \cap D_\infty^{n-j+1}$ est alors de dimension 1 (en posant $D_0^n = D_\infty^n = S$). Si e_j est un vecteur engendrant cette intersection, on vérifie immédiatement que les $e_1, \cdots, e_j$ (resp. $e_{n-j+1}, \cdots, e_n$) forment une base de D_0^j (resp. D_∞^j) pour $1 \leqq j \leqq n$. Le choix de cette base permet de faire opérer G sur S, donc aussi sur l'ensemble des drapeaux de S. On vérifie facilement que Γ (resp. Γ') est alors le stabilisateur de D_0 (resp. D_∞). D'autre part, il est bien connu que G est transitif sur l'ensemble des drapeaux de type donné. Par suite, l'espace homogène G/Γ des classes à droite modulo Γ s'identifie à l'ensemble des drapeaux complets, en faisant correspondre à la classe d'un élément $x \in G$ le transformé de D_0 par x^{-1}. Nous désignerons dans la suite de ce n°, par la même lettre D une classe à droite et le drapeau complet qui lui est ainsi associé.

Soit $D = (D^1, \cdots, D^k)$ un drapeau de type $(\alpha_1, \cdots, \alpha_k)$. Posons:

$$d_0^{ij}(D) = \dim(D^i \cap D_0^j), \tag{9}$$

$$d_\infty^{ij}(D) = \dim(D^i \cap D_\infty^j) \tag{10}$$

pour $1 \leqq i \leqq k$ et $1 \leqq j \leqq n-1$. Possons de plus:

$$s_0(D) = \sum_{i,j} d_0^{ij}(D) \text{ et } s_\infty(D) = \sum_{i,j} d_\infty^{ij}(D). \tag{11}$$

Si D' est un drapeau transformé de D par un élément de Γ (resp. Γ') on a $d_0^{ij}(D') = d_0^{ij}(D)$ (resp. $d_\infty^{ij}(D') = d_\infty^{ij}(D)$), puisque Γ (resp. Γ') laisse fixe D_0 (resp. D_∞). Réciproquement:

LEMME 8. *Le sous-groupe N (resp. N') est transitif sur l'ensemble A des drapeaux D de type $(\alpha_1, \cdots, \alpha_k)$ pour lesquels les nombres $d_0^{ij}(D)$ (resp. $d_\infty^{ij}(D)$) ont, pour $1 \leqq i \leqq k$ et $1 \leqq j \leqq n-1$, des valeurs données d^{ij}.*

Nous démontrerons ce Lemme par récurrence sur n: il est trivial pour $n = 1$. Supposons—le démontré pour les dimensions $< n$. On se ramène aussitot au cas $\alpha_1 > 0$, $\alpha_k < n$ et A non vide, ce que nous supposerons dans la suite. Il existe alors un entier h et un seul compris compris entre 1 et $k + 1$ tel que:

$$d^{i(n-1)} = \alpha_i \qquad \text{pour } 1 \leqq i < h,$$
$$d^{i(n-1)} = \alpha_i - 1 \quad \text{pour } h \leqq i \leqq k.$$

Faisons la démonstration dans le cas de N et des indices $d_0{}^{ij}$, l'autre cas se traitant de la même manière. Soit $D = (D^1, \cdots, D^k) \in A$; si $h \leqq k$, il existe dans D^h une droite V non contenue dans $D_0{}^{n-1}$. Or il est immédiat que N est transitif sur l'ensemble des droites non contenues dans $D_0{}^{n-1}$. On peut donc par une transformation de N envoyer la droite V sur la droite $D_\infty{}^1$. Nous sommes donc ramené à démontrer que N est transitif sur l'ensemble B des drapeaux D tels que $d_0{}^{ij}(D) = d^{ij}$ et que $D^i \supset D_\infty{}^1$ pour $h \leqq i \leqq k$.

Posons $D_1{}^i = D^i \cap D_0{}^{n-1}$: on a $D_1{}^i = D^i$ pour $1 \leqq i < h$ et D^i est, pour $h \leqq i \leqq k$, somme directe de $D_1{}^i$ et de $D_\infty{}^1$. On en déduit que l'application qui au drapeau $D \in B$ fait correspondre le drapeau $D_1 = (D_1{}^1, \cdots, D_1{}^k)$ de l'espace vectoriel à $n - 1$ dimensions $D_0{}^{n-1}$ est une application bijective de B sur l'ensemble B_1 des drapeaux D_1 de type $(\alpha_1, \cdots, \alpha_{h-1}, \alpha_h - 1, \cdots, \alpha_k - 1)$ de $D_0{}^{n-1}$, tels que $d_0{}^{ij}(D_1) = d^{ij}$ pour $1 \leqq i \leqq k$ et $1 \leqq j \leqq n - 1$ (remarquons que l'on a nécessairement $\alpha_h > \alpha_{h-1}$ si $h \leqq k$).

Or, le sous-groupe G_1 de G formé des matrices g_{ij} avec $g_{i1} = g_{1i} = 0$ pour $i > 1$ et $g_{11} = 1$ laisse stables $D_0{}^{n-1}$ et $D_\infty{}^1$ et s'identifie au groupe $SL(n-1, F_q)$ opérant sur l'espace vectoriel à $n - 1$ dimensions $S_1 = D_0{}^{n-1}$ (muni des drapeaux complets "intersections" de D_0 et D_∞ avec S_1). De plus, le sous-groupe $N_1 = N \cap G_1$ s'identifie au sous-groupe des matrices triangulaires supérieures unipotentes de G_1 et l'application $D \rightarrow D_1$ de B sur B_1 commute avec les opérations de N_1. Or l'hypothèse de récurrence entraine que N_1 est transitif sur B_1, d'où le Lemme.

COROLLAIRE. *Soit D un drapeau complet. Les drapeaux complets correspondant aux classes à droite modulo Γ contenues dans la double classe DN sont exactement les drapeaux D' tels que $d_0{}^{ij}(D') = d_0{}^{ij}(D)$.*

C'est évident.

Puisque S est somme directe de $D_0{}^j$ et de $D_\infty{}^{n-j}$, on a, pour tout sous-espace V^i de dimension i:

$$\dim(V^i \cap D_0{}^j) + \dim(V^i \cap D_\infty{}^{n-j}) \leqq i. \tag{12}$$

LEMME 9. *Pour tout drapeau complet D, il existe un drapeau complet D_1 et un seul satisfaisant aux deux conditions suivantes:*

$$d_\infty^{ij}(D_1) = d_\infty^{ij}(D), \tag{13}$$

$$d_\infty^{ij}(D_1) + d_0^{i(n-j)}(D_1) = i \tag{14}$$

pour $1 \leqq i, j \leqq n-1$.

Ici encore, le Lemme est évident si $n = 1$. Supposons—le démontré pour des dimensions $< n$. Il existe un entier k et un seul (avec $1 \leqq k \leqq n$) tel que:

$$\begin{aligned} d_\infty^{(n-1)j}(D) &= j && \text{pour } 1 \leqq j < k, \\ d_\infty^{(n-1)j}(D) &= j-1 && \text{pour } k \leqq j \leqq n-1. \end{aligned}$$

On vérifie aussitôt que l'hyperplan somme directe de D_∞^{k-1} et de D_0^{n-k} (en posant $D_0^0 = D_\infty^0 = \{0\}$) est l'unique hyperplan V satisfaisant aux deux conditions:

$$\dim(V \cap D_\infty^j) = d_\infty^{(n-1)j}(D), \tag{15}$$

$$\dim(V \cap D_\infty^j) + \dim(V \cap D_0^{n-j}) = n-1. \tag{16}$$

D'après le Lemme 8, il existe un élément de N' qui transforme le sous-espace D^{n-1} de dimension $n-1$ du drapeau D donné en l'hyperplan V (grâce à (15)) et par suite transforme le drapeau D en un drapeau complet D' dont le sous-espace de dimension $n-1$ est V. De plus, on a $d_\infty^{ij}(D') = d_\infty^{ij}(D)$: en résumé, on peut se borner à démontrer le Lemme 9 en supposant $D^{n-1} = V$.

D'autre part, le sous-espace de dimension $n-1$ d'un drapeau complet D_1 satisfaisant à (13) et (14) satisfait en particulier à (15) et (16), donc coincide avec V.

Par ailleurs, la formule (16) montre que les drapeaux D_0' et D_∞' intersections avec V des drapeaux D_0 et D_∞ sont (après suppression de $V \cap D_\infty^k$ et de $V \cap D_0^{n-k}$ si $k < n$ et de $V \cap D_\infty^{n-1}$ et de $V \cap D_0^1$ si $k = n$) des drapeaux complets en position générale de $V = D^{n-1}$. L'hypothèse de récurrence entraine donc qu'il existe un drapeau complet $(D_1^1, \cdots, D_1^{n-2})$ et un seul de V tel que:

$$\begin{aligned} &\dim(D_1^i \cap D_\infty^j) = d_\infty^{ij}(D), \\ &\dim(D_1^i \cap D_\infty^j) + \dim(D_1^i \cap D_0^{n-j}) = i \end{aligned}$$

pour $1 \leqq i, j \leqq n-2$. Il est alors clair que le drapeau

$$D_1 = (D_1^1, \cdots, D_1^{n-2}, V)$$

est l'unique drapeau complet satisfaisant à (13) et (14).

COROLLAIRE. *Pour tout drapeau complet D, il existe un drapeau complet D_1 et un seul satisfaisant à la condition* (13) *et tel que pour tout autre drapeau complet D' satisfaisant à* (13), *l'on ait $s_0(D') < s_0(D_1)$. De plus, pour tout drapeau complet D'' tel que $d_0^{ij}(D'') = d_0^{ij}(D_1)$, on a $s_\infty(D'') \leqq s_\infty(D_1)$, l'égalité n'étant réalisée que si $D'' = D_1$.*

La première assertion résulte immédiatement du Lemme 9 et des inégalités (12). La seconde résulte également du Lemme 9 en échangeant les rôles des indices 0 et ∞.

Nous pouvons maintenant démontrer le Lemme 6: nous allons montrer par récurrence sur $s_\infty(D)$ que $f_D \in \mathcal{H}^0$ pour tout drapeau complet D. C'est vrai pour $s_\infty(D) < s_\infty(D_0)$ puisque $s_\infty(D) \geqq s_\infty(D_0)$ pour tout drapeau complet D. Supposons donc que $f_D \in \mathcal{H}^0$ pour tout drapeau D avec $s_\infty(D) < a$ et soit D un drapeau complet avec $s_\infty(D) = a$. D'après le Corollaire du Lemme 9, il existe un drapeau D_1 et un seul parmi les transformés de D par les divers éléments de N', pour lequel $s_0(D_1)$ soit maximum. Par définition même de $\mathcal{H}^0$, il nous suffit de démontrer que $f_{D_1} \in \mathcal{H}^0$. Or, toujours d'après le Corollaire du Lemme 9, on a $s_\infty(D') < s_\infty(D_1)$ pour tout drapeau D' transformé de D_1 par un élément de N et distinct de D_1. L'hypothèse de récurrence entraine donc que l'on a $f_{D'} \in \mathcal{H}^0$ pour $D' \subset D_1 N$ et $D' \neq D_1$. Appliquons alors le Lemme 7: on a:

$$f_{D_1} = a(D_1)^{-1}(\phi(D_1) - \sum a(D') f_{D'}),$$

la sommation étant étendue aux classes à droite modulo Γ (ou aux drapeaux) D' contenues dans $D_1 N$ et distinctes de D_1. Comme $\phi(D_1) \in \mathcal{H}^0$, on en déduit que $f_{D_1} \in \mathcal{H}$, ce qui achève la démonstration du Lemme 6 et donc du Théorème 2.

5. Le cas de $SL(2, P)$. Nous reprenons les notations des n° 2 et 3, mais nous supposons de plus la dimension n égale à 2. Nous avons alors le résultat suivant:

THÉORÈME 3. *Soit M une représentation irréductible de $K = SL(2, \boldsymbol{O})$ dont la restriction à $N \cap K$ ne contient pas la représentation unité. Alors, M est contenue un nombre de fois inférieur à dim M dans toute représentation complètement irréductible de $G = SL(2, P)$.*

Dans le cas $n = 2$, l'application $x \to \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ est un isomorphisme du groupe additif du corps P sur le sous-groupe N. La représentation régulière de N se décompose donc en somme continue des caractères unitaires θ de N, correspondant aux caractères additifs de P. La représentation régulière de G, qui est équivalente à la représentation de G induite par la représentation régulière de N [6], se décompose donc en somme continue des représentations U^θ de G induites par les caractères θ de N. Mais la représentation régulière de G forme à elle seule un système complet de représentations de $\mathfrak{L}(G)$, donc a fortiori de $\mathfrak{L}(M)$. Par suite, les représentations U^θ forment un système complet de représentations de $\mathfrak{L}(M)$. Or si θ est le caractère unité, on voit comme au n° 3, Remarque 1 que la représentation U^θ se décompose en somme continue des représentations U^λ de G, induites par les caractères unitaires de T, que nous avons étudiées au n° 3. En particulier, nous avons vu (n° 3, Remarque 2) que ces représentations ne contenaient pas M, puisque la restriction de M à $K \cap N$ ne contient pas la représentation unité. La représentation de $\mathfrak{L}(M)$ associée à U^θ est donc nulle pour $\theta = 1$ et par suite, les représentations U^θ pour $\theta \neq 1$ forment encore un système complet de représentations de $\mathfrak{L}(M)$.

Considérons la restriction à N de la représentation ${}^TU^\theta$ du groupe T induite par le caractère θ de N. Nous avons vu que N est ouvert et distingué dans T; les doubles classes de T modulo $(N:N)$ sont les mêmes que les classes à gauche par exemple et correspondent biunivoquement, puisque T est le produit semi-direct de N et de Δ, aux éléments $d_m = \begin{pmatrix} \pi^m & 0 \\ 0 & \pi^{-m} \end{pmatrix}$ de Δ (m entier). On a $N = d_m N d_m^{-1}$ et

$$d_m^{-1}\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} d_m = \begin{pmatrix} 1 & 0 \\ \pi^{2m}x & 1 \end{pmatrix}.$$

On déduit alors des théorèmes de G. W. Mackey [5] que la représentation ${}^TU^\theta$ restreinte à N est somme directe discrète des caractères $\theta_m : x \rightarrow \theta(\pi^{2m}x)$ de N (identifié au groupe additif de P).

D'autre part, la représentation U^θ de G est équivalente à la représentation de G induite par le représentation ${}^TU^\theta$ de T (théorème des représentations induites par étages [6]). Comme $G = TK$, la restriction de U^θ à K est équivalente à la représentation de K induite par la restriction à $T \cap K$ de ${}^TU^\theta$. Mais, on a $T \cap K = N \cap K$ et de ce qui précède, on déduit donc que la restriction de U^θ à K se décompose en somme directe discrète des représentations de K induites par les restrictions θ_m' à $N \cap K$ des caractères θ_m de N.

Parmi les caractères θ_m', on trouve le caractère unité une infinité de fois et les autres caractères θ_m' sont deux à deux distincts. C'est évident si $\theta = 1$. Si $\theta \neq 1$, le noyau Q de θ est, puisque P est totalement discontinu, un sous-groupe ouvert du groupe additif de P (identifié à N), distinct de P. Il existe donc un plus petit entier k tel que $\mathfrak{p}^k \subset Q$. Comme l'identification de N avec P envoie $N \cap K$ sur l'anneau $\mathfrak{O}$ des entiers de P, on voit que $\theta_m' = 1$ si et seulement si $2m \geqq k$. Par contre, si $2m < k$, le plus petit entier positif h tel que $\mathfrak{p}^h$ soit contenu dans le noyau de θ_m' est $k - 2m$. Par suite, les caractères θ_m' pour $2m < k$ sont distincts du caractère unité et sont deux à deux distincts.

Soit alors α_m le nombre de fois que la restriction de M à $N \cap K$ contient le caractère θ_m'. Par hypothèse, on a $\alpha_m = 0$ si $\theta_m' = 1$. On a donc $\sum_m \alpha_m \leqq \dim M$.

D'après le théorème de réciprocité de Frobenius, M est contenue α_m fois dans la représentation de K induite par θ_m'. Par suite, M est contenue $\sum \alpha_m$ fois dans la restriction à K de U^θ. Les représentations U^θ forment donc un système complet de représentations de $\mathscr{L}(M)$ et M est contenue au plus $\dim M$ fois dans chaque U^θ: il suffit donc appliquer le résultat fondamental de R. Godement rappelé au n° 1 pour obtenir le Théorème 3.

BIBLIOGRAPHIE.

[1] N. Bourbaki, *Algèbre*, Chapitre VII, Paris, 1952.

[2] F. Bruhat, "Sur les représentations induites des groupes de Lie," *Bulletin de la Société Mathématique de France*, vol. 84 (1956), pp. 97-205.

[3] ———, "Distributions sur un groupe localement compact et applications à l'étude des représentations des groupes $\mathfrak{p}$-adiques," *ibid.*, vol. 89 (1961).

[4] R. Godement, "A theory of spherical functions," *Transactions of the American Mathematical Society*, vol. 73 (1952), pp. 496-556.

[5] G. W. Mackey, "On induced representations of groups," *American Journal of Mathematics*, vol. 73 (1951), pp. 1145-1162.

[6] ———, "Induced representations of locally compact groups," *Annals of Mathematics*, vol. 55 (1952), pp. 101-139.

[7] F. I. Mautner, "Spherical functions over $\mathfrak{p}$-adic fields," *American Journal of Mathematics*, vol. 80 (1958), pp. 441-457.

[8] B. L. Van der Waerden, *Gruppen von linearen Transformationen*, Berlin, 1935.

PATHOLOGIES OF MODULAR ALGEBRAIC SURFACES.*

By DAVID MUMFORD.

The purpose of this note is to present two counterexamples to conjectures about the geometry of algebraic surfaces, which are, on the contrary, true in characteristic zero. Thus if F is a non-singular algebraic surface defined over an algebraically closed field k, one can form the vector spaces

$$H_{0,1} = H^1(F, \Omega^0),$$
$$H_{1,0} = H^0(F, \Omega^1),$$

where Ω^i is the sheaf of regular i-forms. One also has the vector space

$$A_0 = \text{cotangent space to the Albanese Variety } A \text{ of } F \text{ at the origin } 0.$$

Among these vector spaces various maps may be defined regardless of the ground field. First, the canonical map

$$\phi : F \rightarrow A$$

induces a homomorphism

$$\phi^* : A_0 \rightarrow H_{1,0},$$

which Igusa [4] has shown to be one-one. Secondly, if an embedding of F in projective space is fixed, and hence a canonical element h in $H^1(F, \Omega^1)$, then cup product and Serre duality induces a pairing

$$\mathfrak{A} : H_{0,1} \times H_{1,0} \rightarrow k.$$

(See Kodaira [6] and Serre [9]).

Now in the classical case, the usual constructive existence proof of the Albanese variety A shows immediately that ϕ^* is onto (see Weil [12]); while the famous topological results of Lefschetz on the embeddings of varieties in projective space (see Wallace [11], and Kodaira [6]), allow one to conclude that the pairing $\mathfrak{A}$ is non-degenerate. One deduces the "fundamental equalities" of Italian surface theory:

$$\dim A_0 = \dim H_{1,0} = \dim H_{0,1},$$

---

* Received January 4, 1961.

proven first by Poincaré by his method of normal functions in 1910, (Poincaré [8]). A corollary of ϕ^* being onto, combined with the easy proof (valid in all characteristics—see Koizumi [7]) that regular differentials on an Abelian variety are closed, shows that the differentials in $H_{1,0}$ are all closed. This has been generalized by Hodge, and has led ultimately to the result: analytic regular differentials on a Kähler manifold are closed (see Weil [12]).

The question is what extends to the modular, or non-zero characteristic case. Igusa showed, first of all, that ϕ^* is not always onto [5]. Serre showed next that the pairing $\mathfrak{A}$ is not always non-degenerate, since it can happen that $H_{1,0} = (0)$, while $H_{0,1} \neq (0)$, (see [10]). There remain the questions:

(a) Are all differentials in $H_{1,0}$ closed?

(b) Does the pairing $\mathfrak{A}$ have the property that if x in $H_{1,0}$ is such that $\mathfrak{A}(x, y) = 0$ for all y in $H_{0,1}$, then $x = 0$?

The answer to both is no.

I.

To answer (a), we prove (assuming the characteristic $\neq 0$):

THEOREM. *Let F be a non-singular algebraic surface, ω any simple differential on F (i. e. 1-form); then there exists a non-singular surface F^* and a regular map $\phi\colon F^* \to F$ which is separable and algebraic, such that $\phi^*(\omega)$ is regular on F^*.*

Proof. Note first that it is enough to prove:

(#) For all P in F, there exists an open U containing P, a surface F^* and a regular map $\phi\colon F^* \to F$ separable and algebraic such that $\phi^{-1}(U)$ is non-singular, and $\phi^*(\omega)$ is regular on $\phi^{-1}(U)$.

If this is proven, then we can find a finite set U_i^* of open sets covering F and of surfaces F_i^*, and maps $\phi_i\colon F_i^* \to F$ with the above properties. Then let F^* be some non-singular model of the function field of any compositum of $k(F_i^*)$ (compatible with the identification of the common subfields $k(F)$), that dominates the models F_i^* (such exists by Abhyankar [1] and Zariski [13]). Let ϕ be the map from F^* to F. Then for all P in F^*, say $\phi(P)$ in U_i. Then $\phi_i^*(\omega)$ is regular at $\phi_i^{-1}(\phi(P))$, hence $\phi^*(\omega)$ is regular at P.

But in fact it is enough to prove:

(##) Same as (#) except for differentials $\omega = A\,dx$, x a uniformizing parameter at P.

For if at P, $\omega = A\,dx + B\,dy$, then pick F_1^* that does the trick for $A\,dx$ and then F_2^* that does the trick for $B\,dy$, and take a suitable non-singularization of their join as in (#).

But now if $\omega = (A_0/A_1)\,dx$, A_0 and A_1 regular at P, and $A_1 = 0$ at P, consider the extension

$$Z^P + (A_1^P \cdot Z) + (x) = 0, \text{ where } p \text{ is the characteristic.}$$

It follows

$$dx = -A_1^P dZ.$$

Now in the normalization F^* of F in this field extension, there is a unique point P^* above P. Moreover, it is simple since if x, y are uniformizing parameters at P, then Z, y are uniformizing parameters at P^*. Finally,

$$\omega = (A_0/A_1)\,dx = A_0A_1^{p-1}(dx/A_1^p) = -A_0A_1^{p-1}\,dZ.$$

Hence ω is regular at P^*, hence in an open set about P^*. QED

COROLLARY. *There exist algebraic surfaces, non-singular and with a simple regular differential* ω *that is not closed.*

Proof. Take in the above theorem $F = P^2$, the projective plane, and $\omega = x\,dy$. Then the differential $\phi^*(\omega)$ on the covering F^* given by the theorem satisfies the corollary. One must merely note that $d\phi^*(\omega) = \phi^*(d\omega) \neq 0$ as the covering is separable. QED

II.

To answer (b), consider the famous Enriques surface E, which is, in any characteristic, the normalization of the sextic surface E_0 in P^3:

$$0 = x^2y^2z^2 + x^2y^2 + x^2z^2 + y^2z^2 + xyzf_2(x,y,z),$$

where f_2 is a general polynomial of second degree. Its normalization is non-singular and, regardless of characteristic, can be constructed as the join of the graphs of the following set of maps:

$$\phi_1\colon E_0 \to P^1, \text{ given by } xy/z,$$
$$\phi_2\colon E_0 \to P^1, \text{ given by } xz/y,$$
$$\phi_3\colon E_0 \to P^1, \text{ given by } yz/x,$$

as the reader may with some pains verify. It follows that the surface E in characteristic 2 is a specialization of E in characteristic 0, hence has the same p_a (see Hironaka [3]), which has long been known to be 0 (for a modern treatment, see Artin's thesis [2]). On the other hand, the classical theory of adjoint surfaces tells us that canonical divisors on E, as divisors on E_0, must be cut out by $(6-4)=2$nd order forms in P^3 passing through the double lines (see Zariski [14]); in this case, we have a tetrahedron of double lines and such are contained in no quadric. Hence $p_g=0$, hence $H^{0,1}=(0)$.

Now in the remarkable case of characteristic 2, it is also the case that $H^{1,0}\neq(0)$. In fact, let t be a coordinate on P^1; then:

$$\phi_1^*(dt)=\phi_2^*(dt)=\phi_3^*(dt)=d(xyz)$$

is immediately seen to be a regular differential on E.

HARVARD UNIVERSITY.

REFERENCES.

[1] S. Abhyankar, "Local uniformization of algebraic surfaces over ground fields of characteristic $p\neq 0$," *Annals of Mathematics*, vol. 63 (1956), p. 491.

[2] M. Artin, *On Enriques' Surfaces*, Doctoral thesis, Harvard, 1960.

[3] H. Hironaka, "A note on algebraic geometry over ground rings," *Illinois Journal of Mathematics*, vol. 2 (1958), p. 355.

[4] J. I. Igusa, "A fundamental inequality in the Theory of Picard varieties," *Proceedings of the National Academy of Sciences, USA*, vol. 41 (1955), p. 317.

[5] ———, "On some problems in abstract algebraic geometry," *ibid.*, vol. 41 (1955), p. 964.

[6] K. Kodaira and D. C. Spencer, "On a theorem of Lefschetz and the lemma of Enriques-Severi-Zariski," *Proceedings of the National Academy of Sciences, USA*, vol. 39 (1953), p. 1273.

[7] S. Koizumi, "On differential forms of the first kind on algebraic varieties," *Journal of the Mathematical Society of Japan*, vol. 1 (1949), p. 273.

[8] H. Poincaré, "Sur les Courbes Tracee sur les Surfaces Algebriques," *Annales de l'Ecole Normale Supérieure*, vol. 27 (1910), p. ——.

[9] J. P. Serre, "Faisceaux Algebriques Coherents," *Annals of Mathematics*, vol. 61 (1955), p. 197.

[10] ———, "Sur la topologie des varieties algebriques en caracteristique p," *Symposium on Algebraic Topology*, Mexico, 1956.

[11] A. Wallace, *Homology Theory on Algebraic Varieties*, Pergamon Press, 1958.

[12] A. Weil, *Varietes Kahleriennes*, Paris, 1958.

[13] O. Zariski, "Simplified proof for the resolution of singularities of an algebraic surface," *Annals of Mathematics*, vol. 43 (1942), p. 583.

[14] ———, *An Introduction to the Theory of Algebraic Surfaces*, Mimeographed Lecture Notes, Harvard, 1957-8.

SUR LES REPRÉSENTATIONS DES GROUPES CLASSIQUES $\mathfrak{p}$-ADIQUES II.*

par FRANÇOIS BRUHAT.

Dans [3], nous avons démontré quelques résultats sur la théorie des "fonctions sphériques" au sens de Gelfand-Naimark-Godement-Harish-Chandra (voir p. ex. [7]) sur le groupe $G = SL(m, P)$, où P est un corps $\mathfrak{p}$-adique localement compact. Nous avons en particulier montré que si M est une représentation irréductible du sous-groupe compact maximal $SL(m, \mathfrak{O})$ (où $\mathfrak{O}$ est l'anneau des entiers de P) satisfaisant à une certaine condition (S), alors la représentation M est contenue au plus $\dim M$ fois dans la restriction à $K = SL(m, \mathfrak{O})$ de toute représentation complétement irréductible de G dans un espace de Banach. Ceci s'applique en particulier si l'on prend pour M la représentation unité.

Dans ce qui suit, nous étendons ces résultats au cas des groupes symplectique, orthogonal et unitaire. Les démonstrations données dans [3] utilisent tout d'abord une étude détaillée de certains sous-groupes de G (sous-groupe compact maximal, sous-groupe unipotent maximal, etc.) et des décompositions en classes à droite et en doubles classes modulo K. Ces résultats une fois obtenus, on a déduit les théorèmes rappelés plus haut (et des exemples de représentations M satisfaisant à (S)) par des procédés qui ne font plus du tout intervenir la structure de G. Aussi dans ce qui suit, nous établirons en détail pour les différents groupes étudiés les résultats du premier type et nous nous bornerons ensuite à renvoyer à [3] pour en déduire les théorèmes cherchés, en signalant les quelques modifications qu'il faut alors apporter aux démonstrations de [3] pour les rendre valables dans notre nouveau cas.

1. Notations. Nous conservons en général les notations de [3] : on désigne par P un corps valué localement compact non archimédien, par v la valuation discrète normée de P, par $\mathfrak{O}$ l'anneau des entiers de P, par $\mathfrak{p}$ l'idéal maximal de $\mathfrak{O}$, par $\mathfrak{O}^* = \mathfrak{O} - \mathfrak{p}$ le groupe des entiers inversibles, par π une uniformisante (générateur de $\mathfrak{p}$) et par F le corps résiduel $\mathfrak{O}/\mathfrak{p}$. Nous

---

* Received January 9, 1961.

supposerons que F est un corps fini: autrement dit, ou bien P est un corps fini (et $\pi = 0$), ou bien v n'est pas impropre et P est un corps $\mathfrak{p}$-adique.

Nous désignerons par $M_n(P)$ (resp. $M_n(\mathfrak{O})$) l'anneau des matrices carrées d'ordre n à coefficients dans P (resp. $\mathfrak{O}$); par G le groupe linéaire général $GL(m,P)$ des éléments inversibles de $M_m(P)$ (et non $SL(m,P)$ comme dans [3]); par T (resp. T') le sous-groupe de G formé des matrices triangulaires supérieures (resp. inférieures) dont les coefficients diagonaux sont *au signe près* des puissances entières de π; par N (resp. N') le sous-groupe de T (resp. T') formé des matrices unipotentes de T (resp. T'). Enfin K désigne le sous-groupe $GL(m, \mathfrak{O})$ des éléments inversibles de l'anneau $M_m(\mathfrak{O})$, c'est à dire le sous-groupe de G formé des matrices à coefficients entiers dont le déterminant est un entier inversible: K est un sous-groupe *ouvert* et *compact* de G.

Soit $J: x \rightarrow x^J$ un automorphisme involutif de P (qui peut être l'identité). Si $g = (g_{ij})$ est une matrice rectangulaire à coefficients dans P, nous désignerons par g^J la matrice d'éléments $g_{ij}{}^J$ et par g^* la matrice transposée de g^J.

Soit E un espace vectoriel de dimension m sur P et soit ϕ une forme sesquilinéaire réflexive (au sens de [5]) non dégénérée sur E, relative à l'automorphisme J. Nous allons étudier dans ce qui suit certaines propriétés du groupe $G^0 = G(\phi)$ des automorphismes de E qui laissent ϕ invariante: Le choix d'une base de E définit un isomorphisme du groupe G^0 sur un sous-groupe fermé (que nous noterons encore G^0) de G. Par suite, G^0 est un groupe localement compact. Plus précisément, si Φ est la matrice de ϕ par rapport à la base choisie, une matrice g appartient à G^0 si et seulement si elle satisfait à:

$$g^*\Phi g = \Phi. \tag{1}$$

En particulier, on a $(\text{dét}\, g)(\text{dét}\, g)^J = 1$.

On sait ([5], pp. 11-12) qu'on peut se ramener pour l'étude du groupe G^0 à l'un des trois cas suivants (quitte à multiplier ϕ par une constante non nulle). Cependant, nous excluons de notre étude les groupes orthogonaux et unitaires dans le cas où le corps résiduel F est de caractéristique 2. Nous exposerons ces trois cas en supposant P infini, en laissant au lecteur le soin de modifier nos considérations dans le cas où P est fini (il suffit de supprimer dans ce qui suit tout ce qui a trait à π).

Cas I. *J est l'identité et ϕ est bilinéaire alternée.*

La dimension m de E est alors paire ($m = 2n$) et G^0 est le groupe symplectique $Sp(2n,P)$. On sait que tout élément de G^0 est alors de déterminant 1. D'autre part (cf. [1], p. 79), on peut trouver une base $(e_1,\cdots,e_m)$ de E (base symplectique) telle que la matrice Φ de ϕ par rapport à cette base soit égale à

$$\Phi=\begin{pmatrix}0 & s\\ s_1 & 0\end{pmatrix} \text{ avec } \Phi_{ij}=\phi(e_j,e_i), \tag{2}$$

où s est la matrice carrée d'ordre n dont tous les éléments sont nuls sauf ceux situés sur la deuxième diagonale:

$$s=\begin{pmatrix}0 & \cdots & 0 & 1\\ 0 & \cdots & 1 & 0\\ & \cdots & & \\ 1 & \cdots & 0 & 0\end{pmatrix} \tag{3}$$

et où $s_1=-s$.

Cas II. *J est l'identité, F n'est pas de caractéristique* 2 *et ϕ est bilinéaire symétrique. G^0 est alors le groupe orthogonal* $0(P,\phi)$.

Soit n l'indice de ϕ. On sait (cf. [1], § 4) qu'on peut trouver une décomposition de E en somme directe de trois sous-espaces E_1, E_2 et E_3 tels que E_1 et E_3 soient totalement isotropes maximaux (donc de dimension n) et que E_2 soit l'orthogonal du sous-espace non isotrope E_1+E_3. La restriction de ϕ à E_2 est alors anisotrope. Or on sait classifier toutes les formes quadratiques $\phi(x,x)$ anisotropes sur P (cf. [6], p. 54) : leur dimension est $\leqq 4$. D'autre part, le groupe quotient $P^*/(P^*)^2$ des classes d'éléments de P^* modulo les carrés est d'ordre 4 (cf. [8], p. 186) (d'ordre 2 si P est fini). Plus précisément, soit c un élément de $\mathfrak{O}^*$ dont la classe dans F n'est pas un carré: alors les quatre éléments 1, c, π et $c\pi$ forment un système de représentants de $P^*/(P^*)^2$. On peut trouver une base $e_{n1+},\cdots,e_{n+q}$ de E_2 (avec $q=m-2n$ et $0\leqq q\leqq 4$) telle que (après multiplication éventuelle de ϕ par une constante non nulle) la restriction à E_2 de la forme quadratique associée à ϕ soit l'une des formes suivantes (on désigne par $x_1,\cdots,x_q$ les coordonnées d'un point x de E_2) :

II 1	$q=0$	$0,$
II 2	$q=1$	$x_1^2,$
II 3	$q=2$	$x_1^2-cx_2^2,$
II 4	$q=2$	$x_1^2-\pi x_2^2,$
II 5	$q=2$	$x_1^2-c\pi x_2^2,$

II 6	$q=3$	$x_1^2 - cx_2^2 - \pi x_3^2$,
II 7	$q=3$	$x_1^2 - cx_2^2 - c\pi x_3^2$,
II 8	$q=4$	$x_1^2 - cx_2^2 - \pi(x_3^2 - cx_4^2)$.

On sait (cf. [6] p. 55 ou [4] p. 37) et on vérifie d'ailleurs aisément sur les formules précédentes, que si $x \in E_2$ est tel que $\phi(x,x) \in \mathfrak{O}$, alors on a $x_i \in \mathfrak{O}$, et réciproquement (pour $1 \leqq i \leqq q$). Plus généralement, si a est une matrice carrée d'ordre q à coefficients dans P telle que $a^* A a \in M_q(\mathfrak{O})$ (où A désigne la matrice de la restriction de ϕ à E_2 par rapport à la base $e_{n+1}, \cdots, e_{n+q}$), alors $a \in M_q(\mathfrak{O})$. En particulier, la matrice de tout automorphisme de E_2 laissant la restriction de ϕ invariante est nécessairement à coefficients entiers.

Nous poserons $q' = q$ dans les cas II 1, 2 et 3; $q' = 1$ dans les cas II 4 et 5 et $q' = 2$ dans les cas II 6, 7 et 8. Les coefficients diagonaux A_{ii} de la matrice A sont de valuation 0 pour $1 \leqq i \leqq q'$ et de valuation 1 pour $q' < i \leqq q$.

D'autre part, les sous-espaces E_1 et E_3 sont mis en dualité par la forme ϕ. On peut donc trouver une base $(e_1, \cdots, e_n)$ de E_1 et une base $(e_{n+q+1}, \cdots, e_m)$ de E_3 telles que la matrice Φ de ϕ par rapport à la base $(e_1, \cdots, e_m)$ de E prenne la forme:

$$\Phi = \begin{pmatrix} 0 & 0 & s \\ 0 & A & 0 \\ s_1 & 0 & 0 \end{pmatrix}, \tag{4}$$

où A a la même signification que plus haut, où s est donnée par (2) et où $s_1 = s$.

Cas III. *J n'est pas l'identité, F n'est pas de caractéristique 2 et ϕ est hermitienne. G^0 est alors le groupe unitaire $U(P, \phi)$.*

Soit P' le corps des invariants de J: alors P est une extension quadratique de P' et J est l'unique P'-automorphisme de P distinct de l'identité. Posons $\mathfrak{O}' = \mathfrak{O} \cap P'$ et $\mathfrak{p}' = \mathfrak{p} \cap P'$ et soit π' un générateur de l'idéal $\mathfrak{p}'$ de $\mathfrak{O}'$. Soit c' un élément de $\mathfrak{O}'$ dont la classe dans $F' = \mathfrak{O}'/\mathfrak{p}'$ n'est pas un carré: les éléments 1, c', π' et $c'\pi'$ (1 et c' seulement si P est fini) forment un système de représentants de $P'^*/(P'^*)^2$. Par suite, on a $P = P'(\delta^{\frac{1}{2}})$, où δ est l'un des trois éléments c', π' ou $c'\pi'$. Si $\delta = c'$, l'extension P de P' n'est pas ramifiée et on peut prendre $\pi' = \pi$. Si $\delta = \pi'$ ou $c'\pi'$, l'extension P est ramifiée et on peut supposer que $\pi = \delta^{\frac{1}{2}}$. Dans les deux cas, on a $\pi^J = \pm \pi$. De plus, l'anneau $\mathfrak{O}$ est un module libre sur $\mathfrak{O}'$, admettant 1 et $\delta^{\frac{1}{2}}$ comme base, et l'idéal $\mathfrak{p}$ est lui aussi un module libre sur $\mathfrak{O}'$, admettent comme base

$\pi' = \pi$ et $\pi\delta^{\frac{1}{2}}$ dans le cas $\delta = c'$, et π' et $\pi = \delta^{\frac{1}{2}}$ dans le cas ramifié. Pour tout $u \in P$, nous poserons $Ru = \frac{1}{2}(u + u^J)$ et $Iu = (1/2\delta^{\frac{1}{2}})(u - u^J)$: on a $u \in \mathfrak{O}$ si et seulement si Ru et Iu appartiennent à $\mathfrak{O}'$; si P est non ramifiée, on a $u \in \mathfrak{p}$ si et seulement si Ru et Iu appartiennent à $\mathfrak{p}'$, mais si P est ramifiée, $u \in \mathfrak{p}$ équivaut à $Ru \in \mathfrak{p}'$ et $Iu \in \mathfrak{O}'$.

Soit n l'indice de ϕ et posons $q = m - 2n$. On peut comme au cas II, décomposer E en somme directe de trois sous-espaces E_1, E_2 et E_3 tels que E_2 et E_3 soient totalement isotropes maximaux (donc de dimension n) et que E_2 soit l'orthogonal de $E_1 + E_3$. On a nécessairement $q \leqq 2$ et on peut trouver une base orthogonale $e_{n+1}, \cdots, e_{n+q}$ de E_2 telle que la restriction à E_2 de la forme quadratique hermitienne associée à ϕ prenne (après éventuelle multiplication par une constante) une des formes suivantes:

III 1 $\quad q = 0 \quad 0,$

III 2 $\quad q = 1 \quad x_1 x_1^J,$

III 3 $\quad q = 2, \delta = c' \quad x_1 x_1^J + \pi' x_2 x_2^J,$

III 4 $\quad q = 2, \delta = \pi'$ ou $c'\pi' \quad x_1 x_1^J - c' x_2 x_2^J.$

On désignera par A la matrice de la restriction de ϕ à E_2 par rapport à la base choisie. Comme dans le cas II, on montre que pour qu'une matrice $a \in M_q(P)$ soit telle que $a^* A a \in M_q(\mathfrak{O})$, il faut et il suffit que $a \in M_q(\mathfrak{O})$. On posera $q' = q$, sauf dans le cas III 3, où on prendra $q' = 1$.

Enfin, on peut trouver une base $e_1, \cdots, e_n$ de E_1 et une base $e_{n+q+1}, \cdots, e_m$ de E_3 telles que la matrice Φ de ϕ par rapport à la base $e_1, \cdots, e_m$ de E soit encore donnée par (4), avec $s_1 = s$ donnée par (2).

Dans chacun des trois cas, une base $e_1, \cdots, e_m$ de E telle que la matrice Φ de ϕ par rapport à cette base soit donnée par (4) (on par (1) dans le cas symplectique, ce qui peut encore s'écrire sous la forme (4) avec $A =$ matrice vide et $s_1 = -s$) sera appelée une *base de Witt* de E, la décomposition $E = E_1 + E_2 + E_3$ associée étant appelée la décomposition de Witt associée. Il résulte aussitôt du théorème de Witt (cf. [1], p. 71) qu'on passe d'une décomposition de Witt à une autre par un élément de G^0. Par suite, les restrictions de ϕ aux espaces E_2 de deux décompositions de Witt sont équivalentes, ce qui entraine que les matrices de ϕ par rapport à deux bases de Witt de E sont *les mêmes*.

Nous supposerons dans la suite qu'une base de Witt de E a été choisie une fois pour toutes et c'est cette base que nous utilisons pour identifier G^0 à un sous-groupe de G comme nous l'avons dit plus haut.

2. Quelques sous-groupes remarquables de G^0. Nous allons introduire quelques sous-groupes de G^0 qui vont jouer le même rôle que les sous-groupes de G étudies dans [3]. D'une manière générale, si X est un sous-groupe de G, nous poserons:

$$X^0 = X(\phi) = X \cap G^0. \tag{5}$$

Par exemple, le sous-groupe T^0 sera le sous-groupe des matrices triangulaires supérieures apparenant à G^0 et dont les coefficients diagonaux sont au signe près des puissances de π. De même, K^0 est le sous-groupe *ouvert* et *compact* des éléments de G^0 dont les coefficients sont entiers.

Nous désignerons par H le sous-groupe de G formé des matrices qui, une fois décomposées en tableau de matrices correspondant à la décomposition de Witt $E = E_1 + E_2 + E_3$, sont de la forme:

$$g = \begin{pmatrix} a_1 & x & z \\ 0 & a_2 & y \\ 0 & 0 & a_3 \end{pmatrix}, \tag{6}$$

où a_1, a_3 et z par exemple appartiennent à $M_n(P)$. Autrement dit, on a $g \in H$ si et seulement si $g(E_1) = E_1$ et $g(E_1 + E_2) = E_1 + E_2$. Nous allons déterminer les éléments de $H^0 = G^0 \cap H$. Pour cela, calculons $g^*\Phi g$ pour $g \in H$: on trouve:

$$g^*\Phi g = \begin{pmatrix} 0 & 0 & a_1^* s a_3 \\ 0 & a_2^* A a_2 & a_2^* A y + x^* s a_3 \\ a_3^* s_1 a_1 & a_3^* s_1 x + y^* A a_2 & a_3^* s_1 z + y^* A y + z^* s a_3 \end{pmatrix}. \tag{7}$$

D'après (1), on aura $g \in G^0$ si et seulement si les relations suivantes sont satisfaites:

$$a_1^* s a_3 = s, \tag{8}$$

$$a_3^* s_1 a_1 = s_1, \tag{8 bis}$$

$$a_2^* A a_2 = A, \tag{9}$$

$$a_2^* A y + x^* s a_3 = 0, \tag{10}$$

$$a_3^* s_1 x + y^* A a_2 = 0, \tag{10 bis}$$

$$a_3^* s_1 z + y^* A y + z^* s a_3 = 0. \tag{11}$$

Mais (8 bis) est équivalente à (8) et on peut y satisfaire en prenant a_1 arbitraire dans $GL(n, P)$ et en posant $a_3 = s(a_1^*)^{-1}s$. D'autre part, il ne faut faire intervenir (9), (10) et (10 bis) que si A n'est pas la matrice vide, ce qui exclut le case symplectique. Dans les deux autres cas, on a $s_1 = s$ et $A^* = A$, ce qui montre que (10 bis) est équivalente à (10).

D'autre part, l'élément $g \in H$ s'écrit d'une manière et d'une seule sous la forme dt, avec

$$d = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix} \quad \text{et} \quad t = \begin{pmatrix} 1 & \xi & \zeta \\ 0 & 1 & \eta \\ 0 & 0 & 1 \end{pmatrix}.$$

Si $g \in H^0$, alors a_1, a_2 et a_3 satisfont à (8) et (9), ce qui montre que $d \in H^0$. On a donc aussi $t \in H^0$. Mais si l'on remplace g par t dans les formules (8) à (11), celles-ci se réduisent à:

$$s_1\xi + \eta^* A = 0 \quad \text{(dans les cas II et III, } q > 0\text{)}, \tag{12}$$

$$s_1\zeta + \zeta^* s + \eta^* A \eta = 0. \tag{13}$$

Dans le cas symplectique, la condition (12) n'existe pas et (13) se réduit à:

$$-s\zeta + {}^t\zeta s = 0; \tag{13 bis}$$

autrement dit, la matrices $s\zeta$ doit être *symétrique*.

Dans les cas II et III, (12) détermine ξ si l'on se donne η. Quant à (13), elle devient, en posant $\zeta_1 = s\zeta + \frac{1}{2}\eta^* A \eta$:

$$\zeta_1 + \zeta_1^* = 0; \tag{14}$$

autrement dit, ζ_1 doit être *antihermitiene*.

Remarquons enfin que (9) signifie que a_2 appartient au groupe associé à la restriction de ϕ à E_2. En particulier, a_2 est à coefficients entiers et $\text{dét}\, a_2 \in \mathfrak{O}^*$.

Désignons par Γ^0 le sous-groupe des éléments $g \in H^0$ tels que a_1 (donc aussi a_3 d'après (8)) soit triangulaire supérieure. Soit g un élément *unipotent* de Γ^0: alors a_1 et a_3 sont des matrices triangulaires unipotentes. D'autre part, a_2 définit d'après (9) un élément du groupe de la restriction de ϕ à E_2, restriction qui est *anistrope*, et a_2 est évidemment unipotente. Or si ϕ est une forme quadratique ou hermitienne anisotrope sur un espace E de dimension q quelconque sur un corps Q quelconque, le groupe de ϕ ne contient pas d'éléments u unipotents distincts de l'identité: c'est évident si $q \leqq 1$; démontrons donc cette assertion par récurrence sur q: puisque u est unipotent, il existe un élément $f \neq 0$ de E avec $u(f) = f$. Alors E est somme directe orthogonale de la droite engendrée par f et de l'orthogonal E', de dimension

$q-1$, de f. Puisque u conserve f, il conserve aussi E' et sa restriction à E' est unipotente, donc est l'identité d'après l'hypothèse de récurrence.

Donc, si $g \in \Gamma^0$ est unipotent, on a $a_2 = 1$. On en déduit que l'ensemble des matrices unipotentes de Γ^0 est exactement le sous-groupe N^0 des matrices triangulaires supérieures unipotentes de G^0.

Considérons maintenant le sous-groupe $T^0 = T \cap G^0$. On a $N^0 \subset T^0 \subset \Gamma^0$. Si $g \in T^0$, les coefficients diagonaux g_{ii} de g sont par définition de la forme $\epsilon_i \pi^{\alpha_i}$ avec α_i entier naturel et $\epsilon_i = \pm 1$. Puisque a_2 doit être entière, on a $\alpha_i \geqq 0$ pour $n+1 \leqq i \leqq n+q$; mais on a $v(\text{dét}\, a_2) = 0$ et par suite $\alpha_{n+1} + \cdots + \alpha_{n+q} = 0$, ce qui entraine $\alpha_i = 0$ pour $n+1 \leqq i \leqq n+q$. D'autre part, la formule (8) montre que $\epsilon_i \epsilon_{m+1-i} \pi^{\alpha_i} (\pi^J)^{\alpha_{m+1-i}} = 1$ pour $1 \leqq i \leqq n$, d'où $\alpha_{m+1-i} = -\alpha_i$.

Nous désignerons alors par T^{0+} le sous-groupe de T^0 formé des g tels que $g_{ii} = \pi^{\alpha_i}$ pour $1 \leqq i \leqq n$, et $g_{ii} = 1$ pour $n+1 \leqq i \leqq n+q$. On a alors $g_{ii} = (\pi^J)^{-\alpha_{m+1-i}}$ pour $n+q < i \leqq m$. Il est clair que n'importe quel élément de T^0 s'obtient en multipliant un élément de T^{0+} par une matrice diagonale de coefficients diagonaux égaux à ± 1.

Pour tout système $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ de n entiers rationnels on désigne par d_α' la matrice carrée d'ordre n diagonale définie par $(d_\alpha')_{ii} = \pi^{-\alpha_i}$ pour $1 \leqq i \leqq n$; on pose $d_\alpha'' = s(d_\alpha'^*)^{-1}s$: c'est la matrice diagonale définie par $(d_\alpha'')_{ii} = (\pi^J)^{\alpha_{m+1-i}}$. On pose:

$$d_\alpha = \begin{pmatrix} d_\alpha' & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & d_\alpha'' \end{pmatrix}. \tag{15}$$

Quand α décrit Z^n, la matrice d_α décrit un sous-groupe de T^{0+} que nous noterons Δ^0. On vérifie facilement que T^{0+} est *produit semi-direct* du sous-groupe invariant N^0 et de Δ^0.

Nous désignerons par A^+ l'ensemble des $\alpha \in Z^n$ tels que $\alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_n \geqq 0$ et par Δ^{0+} l'ensemble des d_α pour $\alpha \in A^+$.

3. Les classes à droite modulo K^0.

PROPOSITION 1. *On a* $G^0 = T^{0+}K^0$.

Soit $g \in G^0$. On a $(\text{dét}\, g)(\text{dét}\, g)^J = 1$, ce qui entraine que $\text{dét}\, g$ est un entier inversible. Il existe donc un élément k_1 de $K = GL(m, \mathfrak{O})$ tel que $\text{dét}\, g k_1 = 1$. D'après le Lemme 1 de [3], il existe un élément $t \in T$ avec $\text{dét}\, t = 1$ et un élément $k_2 \in SL(m, \mathfrak{O})$ avec $g k_1 = t k_2$. Par suite, g s'écrit sous la forme tk avec $t \in T$, $\text{dét}\, t = 1$ et $k \in K$. Puisque $g \in G^0$, on doit avoir:

$$t^* \Phi t = (k^*)^{-1} \Phi k^{-1} \tag{16}$$

et le second membre de (16) est une matrice à coefficients entiers puisque $k \in GL(m, \mathfrak{O})$. Ecrivons t sous la forme (6) (avec a_i triangulaires supérieures à coefficients diagonaux égaux au signe près à des puissances de π) ; alors $t^*\Phi t$ est donnée par (7). Nous voyons que $a_2{}^*Aa_2$ doit être entière, ce qui entraine que a_2 est elle aussi entière. D'autre part, on a dét $a_i = \pm \pi^{\alpha_i}$, avec α_i entier rationnel, et nous avons $\alpha_2 \geqq 0$, $\alpha_1 + \alpha_3 \geqq 0$ puisque $a_1{}^*sa_3$ est entière (en tenant compte de ce que dét $s \pm 1$ et que $\pi^J = \pm \pi$), et enfin $\alpha_1 + \alpha_2 + \alpha_3 = 0$ puisque dét $t = 1$. On a donc $\alpha_2 = \alpha_1 + \alpha_3 = 0$ et par suite dét $a_2 = \pm 1$, dét$(a_1{}^*sa_3) = \pm 1$. Posons $b = sa_3{}^*sa_1$; ce qui précède montre que b est une matrice triangulaire supérieure à coefficients dans $\mathfrak{O}$, ayant sur la diagonale (au signe près) des puissances entières nécessairement positives de π et de déterminant ± 1: par suite, les coefficients diagonaux de b sont égaux à ± 1.

Nous allons déterminer un élément $h \in T \cap K$ tel que $th^{-1} \in T^{0+}$: on aura alors $g = (th^{-1})(hk)$, d'où $hk \in K \cap G^0 = K^0$ et la Proposition 1 sera démontrée.

Posons tout d'abord:

$$h_1 = \begin{pmatrix} b & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{17}$$

On a $h_1 \in T \cap K$ et:

$$th_1{}^{-1} = \begin{pmatrix} a_1 b^{-1} & x a_2{}^{-1} & z \\ 0 & 1 & y \\ 0 & 0 & a_3 \end{pmatrix}. \tag{18}$$

On a $(a_1 b^{-1})^* sa_3 = s$: autrement dit, nous pouvons supposer en changeant de notations, que dans notre matrice t initiale telle que $g = tk$, on avait d'une part $a_2 = 1$, d'autre part $a_1{}^*sa_3 = s$. En écrivant que $t^*\Phi t$ est à coefficients entiers, on voit de plus que les matrices $u = Ay + x^*sa_3$ et $v = a_3{}^*s_1z + y^*Ay + z^*sa_3$ sont à coefficients entiers. Cherchons alors à déterminer une matrice

$$h_2 = \begin{pmatrix} 1 & \xi & \zeta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{19}$$

à coefficients dans $\mathfrak{O}$ (donc appartenant à $T \cap K$), telle que $th_2 \in T^0$, c'est à dire que $(th_2)^*\Phi th_2 = \Phi$. Un calcul immédiat montre (en utilisant les formules (8) à (11)) qu'il faut et il suffit que ξ et ζ satisfasse à:

$$\xi^* a_1{}^* sa_3 = -(Ay + x^*sa_3), \tag{20}$$

$$a_3{}^*s_1a_1\zeta + \zeta^*a_1{}^*sa_3 = -(a_3{}^*s_1z + y^*Ay + z^*sa_3). \tag{21}$$

Tenant compte de $a_1{}^*sa_3 = s$, on satisfait à (20) en prenant $\xi = -su^*$ (rappelons que u est entière). Quant à (21), elle s'écrit dans le cas symplectique:

$$s\zeta - {}^t(s\zeta) = v, \tag{22}$$

et $v = {}^tzsa_3 - {}^t({}^tzsa_3)$ est une matrice carrée d'ordre n antisymétrique entière, avec des coefficients diagonaux *nuls.* Soit alors w la matrice carrée d'ordre n definie par $w_{ij} = v_{ij}$ pour $i < j$ et $w_{ij} = 0$ pour $i \geqq j$: on a $w - {}^tw = v$ et il suffit de prendre $\zeta = sw$ pour obtenir une matrice entière satisfaisant à (22).

Dans les deux autres cas, on a $s_1 = s$, v est hermitienne entière et (21) s'écrit:

$$s\zeta + (s\zeta)^* = -v, \tag{23}$$

et il suffit de prendre $\zeta = -\frac{1}{2}sv$.

Dans tous les cas, nous avons donc trouvé un élément h_2 de $T \cap K$ tel que $th_2 \in T^0$. Enfin, il existe une matrice diagonale h_3 à coefficients diagonaux égaux ± 1 telle que $th_2h_3 \in T^{0+}$: il est clair que $h_2h_3 \in T \cap K$, ce qui achève la démonstration.

Remarque. On trouvera dans [2], Proposition 15 un résultat analogue pour les groupes simples de Chevalley sur un corps $\mathfrak{p}$-adique.

4. Les réseaux maximaux. Rappelons qu'un *réseau* de l'espace vectoriel E est un sous-$\mathfrak{O}$-module de type fini engendrant l'espace vectoriel E. On sait (cf. p. ex. [6], p. 47) qu'un tel réseau est exactement le $\mathfrak{O}$-module libre engendré par une base de E.

Soit $\mathfrak{L}$ un réseau de E. Considérons l'idéal $\mathfrak{n}(\mathfrak{L})$ du corps P' (avec $P' = P$ dans les cas I et II) engendré par les éléments suivants (où x et y décrivent $\mathfrak{L}$):

dans le cas I: $\phi(x,y)$;

dans le cas II: $\frac{1}{2}\phi(x,x)$ (remarquons que $\mathfrak{n}$ contient alors automatiquement les éléments $\phi(x,y) = \frac{1}{2}(\phi(x+y,x+y) - \phi(x,x) - \phi(y,y))$; d'autre part, le facteur $\frac{1}{2}$ est pour nous sans importance puisque nous avons supposé que $2 \in \mathfrak{O}^*$);

dans le case III: $\frac{1}{2}\phi(x,x)$, $R\phi(x,y)$ et $I\phi(x,y)$ (remarquons que $R\phi(x,y)$ est déjà dans l'idéal engendré par les $\frac{1}{2}\phi(x,x)$ et que ici aussi, le facteur $\frac{1}{2}$ est sans importance).

Nous appelerons *norme* du réseau $\mathfrak{L}$ la borne inférieure λ des valuations des éléments de l'idéal $\mathfrak{n}$: autrement dit, on a $\mathfrak{n} = (\mathfrak{p}')^\lambda$ dans les cas I, II et III non ramifié et $\mathfrak{n} = (\mathfrak{p}')^{\frac{1}{2}\lambda}$ dans le cas III ramifie. Remarquons que $\phi(x, y)$ appartient, pour tous $x, y \in \mathfrak{L}$, à l'idéal $\mathfrak{O}\mathfrak{n}$ de P et que, sauf dans le cas III ramifié, l'idéal engendré par les $\phi(x, y)$ dans P est $\mathfrak{p}^{\lambda}$.

Si $\mathfrak{L}$ est le réseau engendré par une base $f_1, \cdots, f_m$ de E, et si (r_{ij}) est la matrice de ϕ par rapport à cette base $(r_{ij} = \phi(f_j, f_i))$, on vérifié aussitôt que l'idéal $\mathfrak{n}$ est engendré:

dans le cas I par les r_{ij},
dans le cas II par les $\frac{1}{2} r_{ii}$ et r_{ij},
dans le cas III par les $\frac{1}{2} r_{ii}$, les $R r_{ij}$ et les $I r_{ij}$.

Nous dirons qu'on réseau de norme λ est *maximal* s'il est maximal dans l'ensemble des réseaux de norme λ, ordonné par inclusion.

Considérons en particulier le réseau $\mathfrak{L}_0$ engendré par la base de Witt donnée $e_1, \cdots, e_m$, que nous appelerons *réseau initial*: c'est un *réseau maximal de norme* 0. En effet, il est immédiat que $n(\mathfrak{L}_0) = \mathfrak{O}'$, puisque tous les coefficients de la matrice Φ de ϕ sont entiers et que l'un au moins d'entre eux est égal à 1. Soit $\mathfrak{L}$ un réseau de norme 0, contenant $\mathfrak{L}_0$, et soit $x = \sum x_i e_i \in \mathfrak{L}$. On a:

$$\phi(x, e_i) = \pm x_{m+1-i} \text{ pour } 1 \leqq i \leqq n \text{ et } n + q < i \leqq m. \tag{24}$$

Par suite, $x_i \in \mathfrak{O}$ pour $1 \leqq i \leqq n$ et $n + q < i \leqq m$ et

$$y = \sum_{n+1}^{n+q} x_i e_i \in \mathfrak{L}.$$

Comme $y \in E_2$ et que $\phi(y, y)$ doit être entier, on a aussi $x_i \in \mathfrak{O}$ pour $n < i \leqq n + q$ (cf. n° 2). Donc $x \in \mathfrak{L}_0$, ce qui montre bien que $\mathfrak{L}_0$ est maximal.

Nous allons maintenant, en imitant une démonstration donnée par M. Eichler dans le cas orthogonal [6], comparer deux réseaux maximaux: on peut toujours se ramener au cas de normes positives.

THÉORÈME 1. *Soit* λ_j (pour $j = 1, 2$) *un entier naturel* (resp. *un entier naturel pair dans le cas* III *ramifié*). *Soit* μ_j (resp. ν_j) *le plus petit entier naturel inférieur à* $\frac{1}{2}(\lambda_j + 1)$ (resp. $\frac{1}{2}\lambda_j$). *Soit* $\mathfrak{L}_j$ *un réseau maximal parmi les réseaux de norme* $\geqq \lambda_j$. *Supposons* $\lambda_2 \geqq \lambda_1 \geqq 0$. *Alors il existe une base de Witt* $f_1, \cdots f_m$ *de* E *et* n *entiers naturels* $\alpha_1, \cdots, \alpha_n$ *avec* $\alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_n \geqq 0$ *tels que:*

(a) *les vecteurs*

$$\pi^{\lambda_1} f_1, \cdots, \pi^{\lambda_1} f_n, \pi^{\mu_1} f_{n+1}, \cdots, \pi^{\mu_1} f_{n+q'},$$
$$\pi^{\nu_1} f_{n+q'+1}, \cdots, \pi^{\nu_1} f_{n+q'}, f_{n+q+1}, \cdots, f_m$$

forment une base du $\mathfrak{O}$-module $\mathfrak{L}_1$;

(b) *les vecteurs*

$$\pi^{\lambda_2-\alpha_1}f_1, \cdots, \pi^{\lambda_2-\alpha_n}f_n, \pi^{\mu_2}f_{n+1}, \cdots, \pi^{\mu_2}f_{n+q'}$$
$$\pi^{\nu_2}f_{n+q'+1}, \cdots, \pi^{\nu_2}f_{n+q}, \pi^{\alpha_n}f_{n+q+1}, \pi^{\alpha_{n-1}}f_{n+q+2}, \cdots, \pi^{\alpha_1}f_m$$

forment une base du $\mathfrak{O}$-module $\mathfrak{L}_2$.

Nous démontrerons ce théorème par récurrence sur l'indice n de ϕ. Traitons d'abord le cas $n = 0$ d'une forme anisotrope: on peut supposer $m = q > 0$, ce qui exclut le cas I. Nous avons vu que dans le cas anisotrope, la condition $\phi(x,x) \in \mathfrak{O}$ entraine que les coordonnées de x par rapport à une base de Witt sont entières. Par suite, $\mathfrak{L}_0$ est l'unique réseau maximal de norme 0. Soit $\mathfrak{L}$ un réseau maximal parmi les réseaux de norme $\geqq \lambda$. Si λ est pair ($\lambda = 2\mu = 2\nu$), le seul réseau maximal de norme λ est évidemment le réseau $\pi^\mu \mathfrak{L}_0$. Si λ est impair ($\lambda = 2\mu - 1 = 2\nu + 1$), deux cas sont à envisager. Si $q' = q$ (cas II 2 et II 3, III 2 et III 4), la forme $\bar{\phi}$ sur l'espace vectoriel $\mathfrak{L}_0/\mathfrak{p}\mathfrak{L}_0$ obtenue par réduction modulo $\mathfrak{p}$ de la restriction à $\mathfrak{L}$ de ϕ, est anisotrope; par suite, $\phi(x,x) \in \mathfrak{p}$ entraine $x \in \mathfrak{p}\mathfrak{L}_0$ et $\phi(x,x) \in \mathfrak{p}^\lambda$ entraine $x \in \mathfrak{p}^\mu \mathfrak{L}_0$: le réseau $\mathfrak{p}^\mu \mathfrak{L}_0$ est donc l'unique réseau maximal parmi les réseaux de norme $\geqq \lambda$; il est d'ailleurs de norme $\lambda + 1$. Si $q' < q$ (cas II 4 à 8 et cas III 3), la forme $\bar{\phi}$ a pour noyau le sous-espace de $\mathfrak{L}_0/\mathfrak{p}\mathfrak{L}_0$ sous-tendu par les images de $e_{q'+1}, \cdots, e_q$ et sa restriction au sous-espace sous-tendu par les images de $e_1, \cdots, e_{q'}$ est anisotrope. Si $x = \sum x_i e_i$ est tel que $\phi(x) \in \mathfrak{p}$, on a donc $x_1, \cdots, x_{q'} \in \mathfrak{p}$ et $x_{q'+1}, \cdots, x_q \in \mathfrak{O}$, et réciproquement. L'unique réseau maximal de norme λ est le réseau engendré par $\pi^\mu e_1, \cdots, \pi^\mu e_{q'}$ et par $\pi^\nu e_{q'+1}, \cdots, \pi^\nu e_q$. On en déduit aussitot le théorème dans le cas $n = 0$.

Supposons donc le Théorème 1 démontré pour les formes d'indice $< n$ et supposons $n \geqq 1$. On a tout d'abord:

LEMME 1. *Soit $\mathfrak{L}$ un réseau maximal de norme λ et soit x un élément isotrope de $\mathfrak{L}$, tel que $\pi^{-1}x \notin I$. Il existe un élément isotrope x' de $\mathfrak{L}$ tel que $\phi(x,x') = \pi^\lambda$.*

Nous démontrerons ce lemme dans le cas III. Pour les autres cas, il suffit de supprimer les termes en $\delta^{\frac{1}{2}}$ dans ce qui suit, ce qui simplifie un peu la démonstration. Montrons tout d'abord qu'il existe un $y \in \mathfrak{L}$ avec $v(P\phi(x,y)) = \lambda$. Sinon, on aurait $\phi(x,y) = \alpha + \beta\delta^{\frac{1}{2}}$ avec $\alpha \in \mathfrak{O}' \cap \mathfrak{p}^{\lambda+1}$ pour tout $y \in \mathfrak{L}$. Comme $\delta^{\frac{1}{2}}y \in \mathfrak{L}$ et que $\phi(x, \delta^{\frac{1}{2}}y) = -\beta\delta - \alpha\delta^{\frac{1}{2}}$, on aurait aussi $\beta\delta \in \mathfrak{O}' \cap \mathfrak{p}^{\lambda+1}$. Si P est une extension non ramifiée de P', on a $\delta \in \mathfrak{O}'^{*}$ et ceci entraine $\beta \in \mathfrak{O}' \cap \mathfrak{p}^{\lambda+1}$, d'où

$$(25) \qquad \phi(\pi^{-1}x, y) \in \mathfrak{O}' \cap \mathfrak{p}^\lambda + (\mathfrak{O}' \cap \mathfrak{p}^\lambda)\delta^{\frac{1}{2}} \text{ pour tout } y \in \mathfrak{L}.$$

Si P est ramifiée (donc $\pi = \delta^{\frac{1}{2}}$), alors λ est pair et on a $\mathcal{O}' \cap \mathfrak{p}^{\lambda+1} = (\mathfrak{p}')^{\frac{1}{2}\lambda+1} = \mathcal{O}' \cap \mathfrak{p}^{\lambda+2}$. On a donc $\beta \in \mathfrak{p}^{\lambda}$ et $\alpha \in \mathfrak{p}^{\lambda+2}$ et $\phi(\pi^{-1}x, y) = \beta + \pi^{-2}\alpha\delta^{\frac{1}{2}}$ satisfait encore à (25). On vérifie alors immédiatement en utilisant (25) et le fait que x est isotrope que le réseau $\mathcal{L}'$ engendré par $\mathcal{L}$ et $\pi^{-1}x$ est encore de norme $\geqq \lambda$, ce qui contredit la maximalité de $\mathcal{L}$.

Nous avons donc démontré l'existence d'un $y \in \mathcal{L}$ tel que $\phi(x,y) = \pi^{\lambda}(\alpha + \beta\delta^{\frac{1}{2}})$, avec $\alpha \in \mathcal{O}'^{*}$ et $\beta \in \mathcal{O}'$. Mais $\alpha + \beta\delta^{\frac{1}{2}}$ est alors inversible dans $\mathcal{O}$: c'est évident si P est ramifiée ; si P est non ramifiée, on a $\delta = c'$ et $\alpha^2 - c'\beta^2$ n'appartient pas à $\mathfrak{p}$ puisque la classe de c' dans $\mathcal{O}'/\mathfrak{p}$ n'est pas un carré. Par suite, on peut en multipliant y par une constante convenable trouver un $z \in \mathcal{L}$ tel que $\phi(x,z) = \pi^{\lambda}$. On a alors $\phi(z,z) \in \mathfrak{p}^{\lambda}$ et par suite $a = \frac{1}{2}\pi^{-\lambda}\phi(z,z) \in \mathcal{O}$. Il suffit alors de poser $x' = z - ax$ pour trouver l'élément x' cherché, d'où le lemme.

Pour tout vecteur x isotrope de $\mathcal{L}_1$ (resp. $\mathcal{L}_2$), désignons par $t(x)$ (resp. $u(x)$ le plus petit entier naturel tel que $\pi^{t(x)}x$ (resp. $\pi^{u(x)}x$) appartienne à $\mathcal{L}_2$ (resp. $\mathcal{L}_1$) : remarquons que, puisque $\mathcal{L}_1$ est un $\mathcal{O}$-module de type fini et que $\mathcal{L}_2$ engendre E, il existe un entier t tel que $\pi^{t}\mathcal{L}_1 \subset \mathcal{L}_2$; on a donc toujours $t(x) \leqq t$.

Soit x un vecteur isotrope de $\mathcal{L}_1$, tel que $\pi^{-1}x \notin \mathcal{L}_1$ et soit x' isotrope $\in \mathcal{L}_1$ avec $\phi(x,x') = \pi^{\lambda_1}$. On a :

$$\phi(\pi^{t(x)}x, \pi^{t(x')}x') = \pm\, \pi^{t(x)+t(x')}\phi(x,x') \in \mathfrak{p}^{\lambda_2}$$

et par suite :

$$t(x) + t(x') \geqq \lambda_2 - \lambda_1. \tag{26}$$

Mais le vecteur isotrope $y = \pi^{t(x)}x$ appartient à $\mathcal{L}_2$ et $\pi^{-1}y \notin \mathcal{L}_2$: le même raisonnement montre qu'il existe un vecteur isotrope $y' \in \mathcal{L}_2$ avec $\phi(y,y') = \pi^{\lambda_2}$ et tel que $u(y) + u(y') \geqq \lambda_1 - \lambda_2$. Mais on a $u(y) = -t(x)$ et $u(y') = -t(z)$, en posant $z = \pi^{u(y')}y$. On a donc :

$$t(x) + t(z) \leqq \lambda_2 - \lambda_1. \tag{27}$$

Mais z est un élément isotrope de $\mathcal{L}_1$ et $\pi^{-1}z \notin \mathcal{L}_1$: on peut donc faire jouer à z le rôle que jouait x tout à l'heure et trouver un élément z' isotrope dans $\mathcal{L}_1$ tel que :

$$t(z) + t(z') \geqq \lambda_2 - \lambda_1. \tag{28}$$

Supposons alors que x ait été choisi au départ de manière à ce que $t(x)$ ait la plus grande valeur possible (ce qui est loisible puisque $t(x) \leqq t$ pour tout vecteur isotrope $x \in \mathcal{L}_1$). On a alors $t(z') \leqq t(x)$ et les inégalités (27) et (28) ne sont compatibles que si $t(z') = t(x)$ et

$$t(x) + t(z) = \lambda_2 - \lambda_1. \tag{29}$$

On a alors:

$$\phi(x,z)=\phi(\pi^{-t(x)}y,\pi^{-t(z)}y')=\epsilon\pi^{-t(x)-t(z)+\lambda_2}=\epsilon\pi^{\lambda_1}$$

avec $\epsilon=\pm 1$. Posons $f_m=x$, $f_1=\pm\pi^{-\lambda_1}$ et $\alpha_1=t(x)$: on a

$$\alpha_1\geqq\tfrac{1}{2}(t(x)+t(z))\geqq\tfrac{1}{2}(\lambda_2-\lambda_1)\geqq 0.$$

Les éléments f_1 et f_m sont *isotropes* et possèdent les propriétés suivantes (en choisissant convenablement le signe de f_1) :

(30) $$\phi(f_m,f_1)=1,$$

(31) f_m et $\pi^{\lambda_1}f_1$ appartiennent à $\mathfrak{L}_1$,

(32) $\pi^{\alpha_1}f_m$ et $\pi^{\lambda_2-\alpha_1}f_1$ appartiennent à $\mathfrak{L}_2$.

Soit alors E'' le sous-espace engendré par f_1 et f_m et soit E' l'orthogonal de E''. La restriction de ϕ à E' est non dégénérée d'indice $n-1$ et E est somme directe orthogonale de E' et de E'' puisque E'' est non isotrope d'après (30). Posons $\mathfrak{L}_j'=E'\cap\mathfrak{L}_j$ et soit $x\in\mathfrak{L}_1$. On a $x=af_1+bf_m+x'$, avec $x'\in E'$ et

$$a=\phi(f_m,x)\in\mathfrak{p}^{\lambda_1},\qquad b=\phi(x,f_1)\in\pi^{-\lambda_1}\mathfrak{p}^{\lambda_1}=\mathfrak{O}$$

d'après (31). Donc af_1+bf_m appartient au sous-$\mathfrak{O}$-module $\mathfrak{L}_1''$ engendré par f_m et $\pi^{\lambda_1}f_1$, et $x'\in\mathfrak{L}_1'$. Par suite, $\mathfrak{L}_1$ est somme directe orthogonale de $\mathfrak{L}_1'$ et de $\mathfrak{L}_1''$. On montre de même en utilisant (32) que $\mathfrak{L}_2$ est somme directe orthogonale de $\mathfrak{L}_2'$ et du sous-$\mathfrak{O}$-module $\mathfrak{L}_2''$ engendré par $\pi^{\lambda_2-\alpha_1}f_1$ et $\pi^{\alpha_1}f_m$.

Il est alors clair que $\mathfrak{L}_j'$ est un réseau de l'espace E' maximal dans l'ensemble des réseaux de norme $\geqq\lambda_j$ de E'. On peut donc appliquer l'hypothèse de récurrence et trouver une base de Witt de E' soit $f_2,\cdots,f_{m-1}$ et (si $n\geqq 2$) des entiers naturels $\alpha_2\geqq\cdots\geqq\alpha_n\geqq 0$ tels que le réseau $\mathfrak{L}_1'$ (resp. $\mathfrak{L}_2'$) soit engendré par les multiples des vecteurs $f_2,\cdots,f_{m-1}$ qui interviennent dans la condition (a) (resp. (b)) du théorème. Il est alors clair que $f_1,\cdots,f_m$ est une base de Witt de E et que les conditions (a) et (b) sont satisfaites. De plus, nous avons vu que $\alpha_1\geqq 0$ et si $n\geqq 2$, on a $\alpha_1\geqq\alpha_2$ car on a alors $\alpha_2=t(f_{m-1})\leqq t(f_m)=\alpha_1$ d'après le choix même de $f_m=x$.

COROLLAIRE 1. *Soient $\mathfrak{L}_1$ et $\mathfrak{L}_2$ deux réseaux maximaux de norme* 0. *Il existe deux bases de Witt $f_1,\cdots,f_m$ et $g_1,\cdots,g_m$ de E et n entiers naturels $\alpha_1\geqq\cdots\geqq\alpha_n\geqq 0$ tels que:*

(a) *$f_1,\cdots,f_m$ est une base du $\mathfrak{O}$-module $\mathfrak{L}_1$;*

(b) *$g_1,\cdots,g_m$ est une base du $\mathfrak{O}$-module $\mathfrak{L}_2$;*

(c) *on a* $g_i = \pi^{-\alpha_i} f_i$ *pour* $1 \leqq i \leqq n$,
$g_i = f_i$ *pour* $n < i \leqq n+q$,
$g_i = (\pi^J)^{\alpha_i} f_i$ *pour* $n+q < i \leqq m$.

En effet, il suffit d'appliquer le Théorème 1 en faisant $\lambda_1 = \lambda_2 = 0$: on obtient ainsi la base $f_1, \cdots, f_m$ de $\mathfrak{L}_1$ et la condition (b) du Théorème 1 montre que les vecteurs g_i définis en (c) forment une base de $\mathfrak{L}_2$ (compte tenu de $\pi^J = \pm \pi$), et on vérifie immédiatement que c'est une base de Witt de E.

COROLLAIRE 2. *Le groupe G^0 opère transitivement sur les réseaux maximaux de norme* 0.

Avec les notations du Corollaire 1, on vérifie en effet aussitôt que l'application linéaire qui transforme f_i en g_i pour tout i appartient à G^0. On pourrait d'ailleurs énoncer et démontrer ce corollaire en remplaçant "de norme 0" par "de norme λ donnée."

5. Les doubles classes modulo K^0. Le sous-groupe K^0 est exactement le sous-groupe de G^0 stabilisateur du réseau initial $\mathfrak{L}_0$. L'espace homogène G^0/K^0 s'identifie donc à l'ensemble des réseaux maximaux de norme nulle. Nous allons maintenant étudier les doubles classes modulo K^0:

PROPOSITION 2. *Dans toute double classe modulo K^0, il y a un élément de Δ^{0+} et un seul.*

Soit $g \in G^0$ (considéré à la fois et comme automorphisme de E ayant g comme matrice par rapport à la base de Witt initiale). Le transformé $g(\mathfrak{L}_0)$ de $\mathfrak{L}_0$ par l'homomorphisme g est un réseau maximal de norme nulle. Il existe donc deux bases de Witt $(f_1, \cdots, f_m)$ et $(g_1, \cdots, g_m)$ satisfaisant aux conclusions du Corollaire 1 au Théorème 1 (avec $\mathfrak{L}_1 = \mathfrak{L}_0$ et $\mathfrak{L}_2 = g(\mathfrak{L}))$. Puisque le matrices de ϕ par rapport à deux bases de Witt sont les mêmes, l'application linéaire k_1 définis par $k_1(e_j) = f_j$ (pour $1 \leqq j \leqq m$) conserve la forme ϕ et sa matrice (notée encore k_1) par rapport à la base initiale $(e_1, \cdots, e_m)$ appartient à G^0; de plus, comme $(e_1, \cdots, e_m)$ et $(f_1, \cdots, f_m)$ sont des bases du même réseau $\mathfrak{L}_0$, on a $k_1(\mathfrak{L}_0) = \mathfrak{L}_0$ et par suite $k_1 \in K^0$. De même, puisque $(g_1, \cdots, g_m)$ et $(g(e_1), \cdots, g(e_m))$ sont deux bases de Witt engendrant le même réseau $g(\mathfrak{L}_0)$, il existe un automorphisme k_2 de E, conservant ϕ, tel que $k_2(g_j) = g(e_j)$ et la matrice (notée encore k_2) de cet automorphisme *par rapport à la base* $(g_1, \cdots, g_m)$ appartient à K^0. Enfin, considérons l'automorphisme d de E défini par $d(f_j) = g_j$: sa matrice *par* *rapport à la base* $(f_1,\cdots,f_m)$ n'est autre que la matrice d_α définie par (15), avec $\alpha=(\alpha_1,\cdots,\alpha_n)\in A^+$, donc $d_\alpha\in\Delta^{0+}$. Or on a:

$$\begin{aligned} g(e_t) &= \sum_r (k_2)_{rt} g_r = \sum_s \sum_r (k_2)_{rt}(d_\alpha)_{sr} f_s \\ &= \sum_r \sum_s \sum_t (k_2)_{rt}(d_\alpha)_{sr}(k_1)_{ts} e_t \end{aligned}$$

ce qui montre que la *matrice* g est égale au produit des *matrices* $k_1 d_\alpha k_2$ et par suite, $g\in K^0 d_\alpha K^0$, avec $d_\alpha\in\Delta^{0+}$.

Quant à l'unicité de d_α, elle résulte du théorème des diviseurs élémentaires (cf. [3], Lemme 2) : plus précisément, les entiers α_i sont déterminés par la donnée de g comme suit: pour tout r avec $1\leqq r\leqq n$, la somme $-(\alpha_1+\cdots+\alpha_r)$ est la borne inférieure des valuations des mineurs d'ordre r de la matrice g. De plus, $-(\alpha_1+\cdots+\alpha_n)$ est aussi la borne inférieure des valuations des mineurs d'ordre $n+r$ de la matrice g pour $1\leqq r\leqq q$.

COROLLAIRE. *Le sous-groupe K^0 est un sous-groupe compact maximal de G^0.*

Car si H est un sous-groupe de G^0 contenant K^0 et distinct de K^0, alors H contient un élément d_α distinct de l'élément neutre. Or les valuations des coefficients des puissances d'un élément ne sont pas bornées inférieurement et H ne peut pas être compact.

6. Doubles classes et classes à droite modulo $\mathbf{K}^0$. Ordonnons totalement Z^n par l'ordre *opposé* à l'ordre lexicographique: $\beta=(\beta_1,\cdots,\beta_n)$ est $\geqq$ à $\alpha=(\alpha_1,\cdots,\alpha_n)$ si $\beta_i<\alpha_i$ pour le plus petit indice i tel que $\beta_i\neq\alpha_i$.

PROPOSITION 3. *Soit $\alpha\in A^+$ et soit $\beta\in Z^n$. Si $N^0 d_\beta K^0\cap K^0 d_\alpha K^0$ n'est pas vide, alors $\beta\geqq\alpha$. De plus, on a $N^0 d_\alpha K^0\cap K^0 d_\alpha K^0=d_\alpha K^0$.*

Soit en effet $t\in N^0$ tel que $td_\beta\in K^0 d_\alpha K^0$. En considérant le mineur de td_β obtenu en supprimant les $m-r$ dernières lignes et les $m-r$ dernières colonnes, pour $1\leqq r\leqq n$, on déduit de la caractérisation de d_α donnée plus haut que

$$-(\beta_1+\cdots+\beta_n)\geqq-(\alpha_1+\cdots+\alpha_n)\quad\text{pour } 1\leqq r\leqq n$$

d'où $\beta\geqq\alpha$.

Soit maintenant $t\in N^0$ tel que $g=td_\alpha\in K^0 d_\alpha K^0$. La matrice g est de la forme:

$$g=\begin{pmatrix} a_1 & x & z \\ 0 & 1 & y \\ 0 & 0 & a_3 \end{pmatrix}$$

avec:

$$a_1 = \begin{pmatrix} \pi^{-\alpha_1} & \cdot & \cdots & \cdot \\ 0 & \pi^{-\alpha_2} & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & \pi^{-\alpha_n} \end{pmatrix}$$

Considérons pour $1 \leqq i < j \leqq n$, le mineur A_{ij} d'ordre i de g obtenu en supprimant les $m - i$ dernières lignes et les $(m - i + 1)$ dernières colonnes excepté celle d'indice j. On a:

$$v(A_{ij}) = v(g_{ij}) - \sum_{r=1}^{r=i-1} \alpha_r \geqq - \sum_{r=1}^{r=i} \alpha_r$$

d'après la caractérisation des α_r. D'où:

$$v(g_{ij}) \geqq - \alpha_i \quad \text{pour } 1 \leqq i < j \leqq n. \tag{33}$$

on peut alors par récurrence sur j déterminer pour $1 \leqq i < j \leqq n$ des éléments $k_{ij} \in \mathfrak{O}$ tels que:

$$\sum_{r=i-1}^{r=j-1} g_{ir} k_{rj} + g_{ij} = - \pi^{-\alpha_i} k_{ij} \tag{34}$$

le premier membre de (34) étant de valuation $\geqq - \alpha_i$ d'après (33) et l'hypothèse de récurrence (et le fait que les α_i vont en décroissant). Complétons ces k_{ij} en une matrice $k_1 \in SL(n, \mathfrak{O})$ en posant $k_{ii} = 1$ pour $1 \leqq i \leqq n$ et $k_{ij} = 0$ pour $1 \leqq j < i \leqq n$. Posons $k_3 = s(k_1{}^*)^{-1} s$ et

$$k = \begin{pmatrix} k_1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & k_3 \end{pmatrix}.$$

On vérifie immédiatement que $k \in K^0$ et que la matrice $g' = gk$ est de la forme:

$$g' = \begin{pmatrix} d_\alpha' & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & d_\alpha'' \end{pmatrix}. \tag{35}$$

Si $q = 0$, il faut supprimer la deuxième ligne et la deuxième colonne dans le tableau de matrices (35). Si $q > 0$, alors la matrice y' est à coefficients entiers. En effet, ses coefficients sont les coefficients g'_{ij} de g' pour $n + 1 \leqq i \leqq n + q$ et $n + q < j \leqq m$. Considérons pour ces valeurs de i et j le mineur B_{ij} d'ordre $n + 1$ de g' obtenu en supprimant les $n + q$ dernières lignes excepté celle d'indice i et les $n + q$ dernières colonnes excepté celle d'indice j. On a:

$$v(B_{ij}) = v(g'_{ij}) - \sum_{r=1}^{r=1} \alpha_r \geqq - \sum_{r=1}^{r=1} \alpha_r$$

toujours d'après les propriétés des α_r, d'où:

(36) $\qquad v(g'_{ij}) \geqq 0$ pour $n < i \leqq n + q$ et $n + q < j \leqq m$.

Enfin, considérons pour $1 \leqq i \leqq n$ et $n + q < j \leqq m$ le mineur C_{ij} d'ordre n de g' obtenu en supprimant les $n + q$ dernières lignes et les $n + q$ dernières colonnes, excepté celle d'indice j, et aussi la i-ième colonne. On a:

$$v(C_{ij}) = -(\alpha_1 + \cdots + \alpha_{i-1}) - (\alpha_{i+1} + \cdots + \alpha_n) + v(g'_{ij}) \geqq -\sum_{r=1}^{r=n} \alpha_r$$

d'où:

(37) $\qquad v(g'_{ij}) \geqq -\alpha_i$ pour $\mathrm{v} \leqq i \leqq n$ et $n + q < j \leqq m$.

Posons alors:

$$k' = d_\alpha{}^{-1} g' = \begin{pmatrix} 1 & (d_\alpha')^{-1} x' & (d_\alpha')^{-1} z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix}.$$

D'après (36) et (37), les matrices y' et $(d_\alpha')^{-1} z'$ sont entières. Puisque $k' \in G^0$, on a $(d_\alpha')^{-1} x' = -s y'^* A$ (10 bis) et $(d_\alpha')^{-1} x'$ est elle aussi entière. Autrement dit, $k' \in K^0$ et par suite, $g = g' k^{-1} = d_\alpha k' k^{-1} \in d_\alpha K^0$, se qui achève la démonstration.

7. Le résultat principal. Soit M une représentation irréductible du sous-groupe compact K^0 de G^0. Rappelons qu'on désigne par $\mathcal{L}(M)$ l'algèbre (pour la convolution) des fonctions continues à support compact sur G^0 qui se transforment suivant M (resp. suivant la représentation $\bar{M}$ conjuguée de M) par la restriction à K^0 de la représentation régulière gauche (resp. droite) de G^0 (cf. [7] et [3], n° 1).

Soit λ un caractère unitaire du groupe abélien Δ^0. Comme Δ^0 s'identifie au groupe quotient T^{0+}/N^0, on peut considérer λ comme un caractère de T^{0+}. Soit U^λ la représentation unitaire de G^0 induite par le caractère λ de T^{0+} et soit $(U^\lambda)^M$ la représentation de $\mathcal{L}(M)$ associée à U^λ (cf. [3], n° 1).

THÉORÈME 2. *Soit M une représentation irréductible de K^0 satisfaisant à la condition suivante:*

(S) *les transformés par les opérateurs M_x pour $x \in K^0 \cap N'^0$ des vecteurs invariants par les opérateurs M_y pour $y \in K^0 \cap N^0$ forment un ensemble total dans l'espace de la représentation M.*

Alors les représentations $(U^\lambda)^M$ forment, quand λ décrit le groupe dual de Δ^0, un système complet de représentations de l'algèbre $\mathcal{L}(M)$.

La démonstration donnée dans [3], n° 3 du résultat analogue pour le groupe $G = SL(m, P)$ ([3], Théorème 1) s'applique sans aucun changement, les Proposition 1, 2 et 3 ci-dessus remplaçant les Lemmes 1, 2 et 3 de [3]. On déduit aussi du Théorème 2 les corollaires suivants, exactement comme dans [3]:

Corollaire 1. *Soit M une représentation irréductible de K^0 satisfaisant à la condition* (S). *Alors M est contenue au plus* $\dim M$ *fois dans toute représentation complètement irréductible de G^0 dans un espace de Banach.*

Corollaire 2. *La représentation unité de K^0 est contenue au plus une fois dans toute représentation complètement irréductible de G^0.*

Corollaire 3. *Si M est la représentation unité de K^0, l'algèbre $\mathfrak{L}(M)$ est commutative.*

8. Exemples de représentations satisfaisant à la condition (S). Cas des corps finis. Dans ce n°, nous supposerons que P est un corps *fini* (donc $\pi = 0$). On a alors $G^0 = K^0$ et il est clair que toute représentation M de K^0 satisfait au Corollaire 1 du Théorème 2, et même à beaucoup mieux! Cependant, M ne satisfait pas nécessairement pas à la condition (S), car (S) entraine évidemment que la restriction de M à T^0 contient la représentation unité. Nous allons démontrer la réciproque.

Pour cela, nous allons interpréter géométriquement les classes à droite modulo Γ^0 et les doubles classes modulo $(\Gamma^0 : N^0)$. Nous appelerons *drapeau isotrope* de type $(\alpha_1, \cdots, \alpha_k)$ dans l'espace E (où les α_i sont des entiers naturels avec $0 \leqq \alpha_1 \leqq \cdots \leqq \alpha_k \leqq n$) une famille de k sous-espaces totalement isotropes $D^1, \cdots, D^k$ avec $\dim D^i = \alpha_i$ et $D^1 \subset \cdots \subset D^k$. Nous appelerons *drapeau isotrope complet* un drapeau isotrope de type $(1, 2, \cdots, n)$. A un drapeau isotrope complet, nous associerons le drapeau $(D^1, \cdots, D^n, D^{n+q}, \cdots, D^{m-1})$ où D^i est, pour $n + q \leqq i \leqq m - 1$, l'orthogonal de D^{m-i}. On a encore $\dim D^i = i$ pour $i \geqq n + q$ et $D^n \subset D^{n+q} \subset \cdots \subset D^{m-1}$ puisque D^n est totalement isotrope.

En particulier, nous désignerons par D_0 (resp. D_∞) le drapeau isotrope complet obtenu en prenant pour $D_0{}^i$ (resp. $D_\infty{}^i$) (pour $1 \leqq i \leqq n$) le sous-espace de E engendré par $e_1, \cdots, e_i$ (resp. $e_{m+1-i}, \cdots, e_m$). Il est clair que $D_0{}^i$ (resp. $D_\infty{}^i$) est encore engendré par $e_1, \cdots, e_i$ (resp. $e_{m+1-i}, \cdots, e_m$) pour $n + q \leqq i \leqq m - 1$.

Let groupe G^0 opère évidemment sur l'ensemble des drapeaux isotropes de type donné et même y opère transitivement d'après le théorème de Witt (cf. [1], p. 71). D'autre part, le stabilisateur du drapeau D_0 n'est autre que le sous-groupe Γ^0: on a en effet $D_0^n = E_1$ et $D_0^{n+q} = E_1 + E_2$, ce qui entraine que le stabilisateur de D_0 est contenu dans le sous-groupe H^0 du n° 2; il suffit alors de remarquer que le stabilisateur dans le groupe des automorphismes de E_1 du drapeau D_0, considéré comme drapeau de l'espace E_1, n'est autre que le sous-groupe des matrices triangulaires supérieures (par rapport à la base $e_1, \cdots, e_n$ de E_1). On a évidemment un résultat analogue pour le drapeau D_∞: en particulier N'^0 est contenu dans le stabilisateur de D_∞.

L'espace homogène G°/Γ^0 des classes à droite modulo Γ^0 s'identifie donc à l'ensemble des drapeaux isotropes complets, en faisant correspondre à la classe $\Gamma^0 x$ d'un élément x de G^0 le transformé de D_0 par x^{-1}. Nous désignerons dans ce qui suit par la même lettre D une classe à droite modulo Γ^0 et le drapeau isotrope complet qui lui correspond.

Soit D un drapeau isotrope de type $(\alpha_1, \cdots, \alpha_k)$. Posons:

$$d_0^{ij} = \dim(D^i \cap D_0^j), \tag{38}$$

$$d_\infty^{ij} = \dim(D^i \cap D_\infty^j) \tag{39}$$

pour $1 \leqq i \leqq k$ et $1 \leqq j \leqq n$ ou $n + q \leqq j < m$.

PROPOSITION 4. *Le sous-groupe* N^0 (resp. N'^0) *est transitif sur l'ensemble* A *des drapeaux isotropes de type donné* $(\alpha_1, \cdots, \alpha_k)$ *pour lesquels les nombres* d_0^{ij} (resp. d_∞^{ij}) *ont des valeurs données* d^{ij}.

Nous ferons la démonstration pour le sous-groupe N^0. La proposition est triviale pour $n = 0$. Nous ferons donc la démonstration par récurrence sur l'indice n de ϕ. On peut toujours supposer $\alpha_1 > 0$ et A non vide.

Supposons tout d'abord $d^{kn} = \alpha_k$, autrement dit on a $D^k \subset D_0^n$ pour tout $D \in A$. Si D_1 et D_2 appartiennent à A, on peut alors ([3], Lemme 8) trouver un automorphisme de $E_1 = D_0^n$ dont la matrice a_1 par rapport à la base $e_1, \cdots, e_n$ soit triangulaire supérieure unipotente, et qui envoie D_1 sur D_2. Posons $a_3 = s(a_1^*)^{-1}s$ et

$$t = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a_3 \end{pmatrix}.$$

On a $t \in N^0$ et t envoie D_1 sur D_2.

Si maintenant $d^{kn} < \alpha_k$, il existe un indice i avec $1 \leqq i \leqq k$ tel que $d^{jn} = \alpha_j$ pour $1 \leqq j < i$ et $d^{in} < \alpha_i$. On a alors $D^i \not\subset D_0^n$ pour tout $D \in A$ et par suite $D^i \not\subset D_0^{n+q}$, car tout sous-espace totalement isotrope de D_0^{n+q} est contenu dans $D_0{}^n$ puisque $D_0{}^{n+q}$ est somme directe orthogonale de $D_0{}^n = E_1$ et de E_2 et que la forme ϕ est nulle sur E_1 et anisotrope sur E_2.

Soit alors j le plus grand entier (avec $n + q < j \leqq m$) tel que $d^{i(j-1)} < \alpha_i$: on a $D^i \not\subset D_0{}^{j-1}$ mais $D^i \subset D_0{}^j$ (avec $D_0{}^m = E$). Soit $x \in D^i$ mais $x \notin D_0{}^{j-1}$: alors x n'est pas orthogonal à $D_0{}^{m-j+1}$, mais est orthogonal à $D_0{}^{m-j}$. Posons:

$$\phi(x, e_r) = \lambda_r \quad \text{pour } 1 \leqq r \leqq n. \tag{40}$$

On a donc $\lambda_r = 0$ pour $1 \leqq r \leqq m - j$ et $\lambda_{m-j+1} \neq 0$: quitte à multiplier x par une constante convenable, on peut même supposer que $\lambda_{m-j+1} = 1$. Posons:

$$y = e_j + \lambda_{m-j+2} e_{j-1} + \cdots + \lambda_n e_{n+q+1}. \tag{41}$$

On a $\phi(x, e_r) = \phi(y, e_r)$ pour $1 \leqq r \leqq n$ (d'après (4)). Considérons alors le sous-espace W_1 (resp. W_2) somme directe de $D_0{}^n$ et de la droite engendrée par x (resp. y). Comme x et y sont isotropes, l'application linéaire de W_1 sur W_2 qui se réduit à l'identité sur $D_0{}^n$ et envoie x sur y transforme la restriction de ϕ à W_1 en la restriction de ϕ à W_2. D'après le théorème de Witt, il existe donc un élément $g \in G^0$ avec $g = 1$ sur $D_0{}^n$ et $g(x) = y$. Puisque le stabilisateur de D_0 est Γ^0, on a $g \in \Gamma^0$ et la matrice g est de la forme:

$$g = \begin{pmatrix} 1 & \xi & \zeta \\ 0 & a_2 & \eta \\ 0 & 0 & 1 \end{pmatrix}.$$

La matrice

$$h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

appartient aussi à G^0 (cf. n° 2) et on a $h^{-1}(y) = y$. Quitte à remplacer g par $h^{-1}g$, on peut donc supposer que $a_2 = 1$, et alors $g \in N^0$. De plus, il existe d'après (41) un automorphisme de E_3 de matrice b_3 triangulaire supérieure unipotente, qui envoie y sur e_j. Posons $b_1 = s(b_3{}^*)^{-1}s$ et

$$g' = \begin{pmatrix} b_1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b_3 \end{pmatrix}.$$

L'élément g' de G^0 appartient à G^0 et $g'g \in N^0$ envoie D^1 sur un sous-espace totalement isotrope contenant e_j.

En résumé, nous sommes ramené à démontrer que deux éléments de l'ensemble B des drapeaux $\in A$ et tels que $e_j \in D^i$, peuvent être transformés l'un en l'autre par un élément de N^0. Or, considérons le sous-espace E^j de dimension $m-2$ engendré par les vecteurs e_r excepté e_j et e_{m+1-j}: ces vecteurs forment une base de Witt de E^j pour la restriction ϕ' de ϕ à E^j, qui est d'ailleurs d'indice $n-1$. Le sous-groupe G'^0 de G^0 laissant invariant E^j, e_j et e_{m+1-j} s'identité au groupe de la forme ϕ' et le sous-groupe $N^0 \cap G'^0$ de G'^0 est l'analogue de N^0. Soit $D \in B$; posons $D'^r = D^r \cap E^j$. Les sous-espaces $D^1, \cdots, D^{i-1}$ sont contenus dans l'intersection de $D_0{}^n$ avec l'orthogonal de e_j (puisque D^i est totalement isotrope et contient e_j et D^r pour $r < i$), donc dans E^j et on a $D'^r = D^r$ pour $1 \leqq r < i$. Quant aux sous-espaces $D^i, \cdots, D^k$, ils sont contenus dans l'orthogonal de e_j et contiennent e_j: ils sont donc somme directe de la droite engendrée par e_j et de leurs intersections $D'^i, \cdots, D'^k$ avec E^j. Par suite, l'application $D \to D'$ est bijective de B sur l'ensemble B' des drapeaux isotropes de type $(\alpha_1, \cdots, \alpha_{i-1}, \alpha_i - 1, \cdots, \alpha_k - 1)$ de E^j dont les dimensions d'intersections avec les espaces $D_0{}^n \cap E^j$ (pour $1 \leqq r \leqq n$ et $n + q \leqq r < m$) ont des valeurs convenables fixées et qu'il serait facile d'écrire. Enfin, il est clair que les opérations de $G'^0 \cap N^0$ dans B et dans B' "commutent" avec l'application $D \to D'$: il suffit donc d'appliquer l'hypothèse de récurrence pour achever la démonstration de la Proposition 4.

COROLLAIRE. *Soit D un drapeau isotrope complet; notons encore D la classe à droite modulo Γ^0 qu'il définit. Les classes à droite modulo Γ^0 contenues dans la double classe DN^0 correspondent exactement aux drapeaux isotropes complets D' tels que $d_0{}^{ij}(D') = d_0{}^{ij}(D)$ pour $1 \leqq i \leqq n$ et $1 \leqq j \leqq n$ ou $n + q \leqq j < m$.*

PROPOSITION 5. *Soit D un drapeau isotrope complet. Il existe un drapeau isotrope complet D' et un seul satisfaisant aux conditions suivantes:*

$$d_0{}^{ij}(D') = d_0{}^{ij}(D), \tag{42}$$

$$d_\infty{}^{ij}(D') + d_0{}^{i(m-j)}(D') = i \tag{43}$$

pour $1 \leqq i \leqq n$ et $1 \leqq j \leqq n$ ou $n + q \leqq j < m$.

Ici encore la proposition est triviale si $n = 0$ et nous ferons la démonstration par récurrence sur l'indice n de ϕ. Considérons la droite isotrope D^1: il existe un entier j et un seul avec $1 \leqq j \leqq n$ ou $n + q < j \leqq m$ tel que $D^1 \subset D_0{}^r$ pour $j \leqq r < m$ et $D^1 \not\subset D_0{}^r$ pour $1 \leqq r < j$, autrement dit, tel que

$$d_0{}^{1r}(D) = 1 \text{ pour } j \leqq r < m \text{ et } d_0{}^{1r}(D) = 0 \text{ pour } 1 \leqq r < j \tag{44}$$

La droite V_j engendrée par e_j satisfait à:

$$\dim(V_j \cap D_0{}^r) = d_0{}^{1r}(D), \tag{45}$$

$$\dim(V_j \cap D_0{}^r) + \dim(V_j \cap D_\infty{}^{m-r}) = 1 \tag{46}$$

quel que soit r, et on vérifie facilement que c'est l'unique droite satisfaisant à (45) et (46). De plus, d'après (45) et la Proposition 4, il existe un élément $g \in N^0$ qui transforme D^1 en V_j. Cet élément transforme le drapeau donné D en un drapeau ayant mêmes nombres $d_0{}^{ir}$ (puisque N^0 invarie D_0) ; on peut donc supposer pour la suite de la démonstration que $D^1 = V_j$. De plus, le sous-espace D'^1 de dimension 1 d'un drapeau isotrope complet D' satisfaisant à (42) et (43) satisfait nécessairement à (45) et (46), donc coincide avec $V_j = D^1$. Un tel drapeau D' est alors contenu dans l'orthogonal de V_j, c'est à dire dans le sous-espace engendré par les e_r excepté e_{m+1-j}. Désignons alors comme plus haut, par E^j le sous-espace engendré par les e_r excepté e_j et e_{m+1-j}. L'espace D^r (resp. D'^r) est totalement isotrope et contient V_j: on en déduit que D^r (resp. D'^r) est somme directe de V_j et de $C^{r-1} = D^r \cap E^j$ (resp. $C'^{r-1} = D'^r \cap E^j$).

Considérons alors le drapeau $C = (C^1, \cdots, C^{n-1})$ de l'espace E^j: c'est un drapeau isotrope complet de E^j et l'hypothèse de récurrence entraine qu'il existe un drapeau isotrope complet C' et un seul dans E^j tel que:

$$\dim(C'^i \cap D_0{}^r) = \dim(C^i \cap D_0{}^r) = \begin{cases} d_0{}^{ir} - 1 & \text{pour } j \leqq r < m \\ d_0{}^{ir} & \text{pour } 1 \leqq r < j, \end{cases}$$
$$\dim(C'^i \cap D_0{}^r) + \dim(C'^i \cap D^{m-r}) = i$$

pour $1 \leqq i \leqq n-1$.

Il est alors clair que le drapeau D', où D'^i est la somme directe de V_j et de C'^{i-1} (pour $1 \leqq i \leqq n$, en posant $C'^0 = \{0\}$), est l'unique drapeau isotrope complet satisfaisant à (42) et (43), d'où la Proposition 5.

Les Propositions 4 et 5 sont l'analogue des Lemmes 8 et 9 de [3]. On en déduit comme dans [3] le résultat suivant:

PROPOSITION 6. *Si P est un corps fini, toute représentation irréductible M de $G^0 = K^0$ dont la restriction à N^0 contient la représentation unité, satisfait à la condition* (S).

Nous nous bornerons à indiquer sommairement les modifications qu'il faut apporter à la démonstration donnée dans [3] pour la rendre valable dans notre nouveau cas. Tout d'abord, on se ramène exactement comme dans [3] (en utilisant le théorème de réciprocité de Frobenius) à montrer que la représentation U de G^0 *induite* par la représentation unité de N^0 satisfait à (S). Comme N^0 est distingué dans Γ^0, cette représentation U se décompose en somme directe des représentations U^λ induites par les diverses représentations irréductibles λ de Γ^0 triviales sur N^0 (chacune intervenant un nombre de fois égal à la dimension de λ). Il suffit alors de démontrer que chaque U^λ satisfait à (S) (cf. Lemme 6 de [3]), ce qui se démontre comme dans [3], en remplaçant les Lemmes 8 et 9 de [3] par les Propositions 4 et 5. Le seul point à modifier est le Lemme 7 de [3], qu'il faut remplacer par ce qui suit. Soit $C = \Gamma^0 x N^0$ une double classe modulo $(\Gamma^0 : N^0)$, et soit H_C le sous-espace de l'espace H^λ de la représentation U^λ formé des fonctions sur G^0 (à valeurs dans l'espace de λ et satisfaisant à $f(\xi y) = \lambda(\xi) f(y)$ pour tout $y \in G^0$ et tout $\xi \in \Gamma^0$) à support contenu dans C. Alors H_C est évidemment invariant par N^0 (qui opère dans H^λ par translations à droite) et pour avoir l'équivalent du Lemme 7 de [3], il suffit de montrer que H_C contient $r = \dim \lambda$ éléments linéairement indépendants et invariants par N^0. Or (cf. [9]), la représentation de N^0 dans H_C est équivalente à la représentation de N^0 induite par la représentation λ_x: $t \to \lambda(xtx^{-1})$ du sous-groupe $N^0 \cap x^{-1}\Gamma^0 x$ de N^0. Mais si $t \in N^0 \cap x^{-1}\Gamma^0 x$, alors t est une matrice *unipotente* de Γ^0 et par suite (n° 2) appartient à N^0. Par suite, λ_x est équivalente à r fois la représentation unité et le théorème de Frobenius entraine que la représentation de N_0 dans H_C contient r fois la représentation unité de N^0.

9. Exemples de représentations satisfaisant à (S). Cas général. Supposons maintenant P infini. Nous pouvons considérer K^0 comme un groupe d'automorphismes du $\mathfrak{O}$-module $\mathfrak{L}_0$, conservant le sous-module $\mathfrak{p}\mathfrak{L}_0$. Tout élément $k \in K^0$ définit donc un automorphisme $\bar{k}$ de l'espace vectoriel $\bar{E} = \mathfrak{L}_0/\mathfrak{p}\mathfrak{L}_0$ de dimension m sur le corps résiduel F. Comme la forme ϕ prend des valeurs entières sur $\mathfrak{L}_0$, on en déduit par réduction modulo $\mathfrak{p}$ une forme $\bar{\phi}$ sur $\bar{E}$ et il est clair que l'application $k \to \bar{k}$ est un homomorphisme de K^0 dans le groupe $G(\bar{\phi})$ des automorphismes de $\bar{E}$ conservant $\bar{\phi}$. Remarquons que $\bar{\phi}$ est une forme bilinéaire alternée dans le cas I, bilinéaire symétrique dans les cas II et III ramifié et sesquilinéaire hermitienne dans le cas III non ramifié. De plus, $\bar{\phi}$ est non dégénérée, excepté dans les cas II 4 à 8 et III 3 : nous exclurons pour l'intant ces six cas et supposerons $\bar{\phi}$ non dégénérée; cela signifie encore que l'inverse Φ^{-1} de la matrice Φ est entière.

Montrons qu'alors l'image de K^0 est $G(\bar{\phi})$ tout entier. Il suffit évidemment de montrer que si une matrice $g \in M_n(\mathfrak{O})$ satisfait à

$$g^* \Phi g \equiv \Phi \mod \mathfrak{p} \tag{47}$$

alors il existe une matrice $g' \in K^0$ avec $g' \equiv g \mod \mathfrak{p}$. Nous allons déterminer par récurrence sur j une suite d'éléments $g_j \in M_m(\mathfrak{O})$, satisfaisant à (pour $j \geqq 0$) :

$$g_j \equiv g \mod \mathfrak{p}, \tag{48}$$

$$g_{j+1} \equiv g_j \quad \bmod \mathfrak{p}^{j+1}, \tag{49}$$

$$g_{j+1}{}^*\Phi g_{j+1} \equiv \Phi \quad \bmod \mathfrak{p}^{j+1}. \tag{50}$$

Alors les matrices g_j convergeront vers l'élément cherché g'. D'après (47), on peut prendre $g_0 = g$. Supposons les g_r déterminées pour $r \leqq j$ (avec $j \geqq 0$ et cherchons g_{j+1} sous la forme:

$$g_{j+1} = g_j + \pi^{j+1}h$$

avec $h \in M_m(\mathfrak{O})$, se qui entraine (48) et (49). On a:

$$g_{j+1}{}^*\Phi g_{j+1} = g_j{}^*\Phi g_j + (\pi^J)^{j+1}h^*\Phi g_j + \pi^{j+1}g_j{}^*\Phi h + (\pi\pi^J)^{j+1}h^*\Phi h.$$

Posons:

$$a = \pi^{-(j+1)}(g_j{}^*\Phi g_j - \Phi).$$

D'après l'hypothèse de récurrence, on a $a \in M_m(\mathfrak{O})$ et pour que g_{j+1} satisfasse à (50), il faut et il suffit que h satisfasse à:

$$a + \epsilon^{j+1}h^*\Phi g_j + g_j{}^*\Phi h \equiv 0 \quad \bmod \mathfrak{p} \tag{51}$$

avec $\epsilon = 1$ si $\pi = \pi^J$ et $\epsilon = -1$ si $\pi^J = -\pi$.

Dans le cas I, on vérifie facilement que la matrice a est alternée; désignons par b la matrice définie par $b_{rs} = a_{rs}$ pour $r \leqq s$ et $b_{rs} = 0$ pour $r \geqq s$: on a $b + b^* = a$. D'autre part, la relation (50) (en remplaçant j par $j-1$) entraine (dans tous les cas) $(\text{dét}\, g)(\text{dét}\, g_j)^J \equiv \bmod \mathfrak{p}$ et par suite $g_j \in GL(m, \mathfrak{O})$. Il suffit alors de poser:

$$h = -\Phi^{-1}(g_j{}^*)^{-1}b$$

pour satisfaire à (51).

Dans les cas II ou III, on a $a^* = \epsilon^{j+1}a$ et 2 est inversible dans $\mathfrak{O}$. Il suffit alors de poser:

$$h = -\tfrac{1}{2}\Phi^{-1}(g_j{}^*)^{-1}a$$

pour satisfaire à (51).

D'autre part, on vérifie très facilement en utilisant les conditions (12) à (14) du n° 2 que l'image de N^0 (resp. N'^0) dans $G(\bar{\phi})$ est exactement le sous-groupe $N(\bar{\phi})$ (resp. $N'(\bar{\phi})$) des matrices triangulaires supérieures (resp. inférieures) unipotentes de $G(\bar{\phi})$ (c'est à dire l'analogue de N^0 (resp. N'^0) pour le groupe $G(\bar{\phi})$). Disons alors qu'une représentation M de K^0 provient d'une représentation de $G(\bar{\phi})$ s'il existe une représentation M_1 de $G(\bar{\phi})$ telle que $M(k) = M_1(\bar{k})$ pour tout $k \in K^0$, autrement dit si M est triviale sur le sous-groupe des matrices congrues à l'identité modulo $\mathfrak{p}$: avec cette terminologie, on déduit immédiatement de la Proposition 6 le:

THÉORÈME 3. *Si la forme* $\bar{\phi}$ *est non dégénérée, toute représentation irréductible de* K^0 *provenant d'une représentation de* $G(\bar{\phi})$ *et dont la restriction à* $K^0 \cap N^0$ *contient la représentation unité, satisfait à la condition* (S).

Dans le cas où $\bar{\phi}$ est dégénérée (ce qui exclut le cas III, ramifié) l'image de K^0 n'est plus $G(\bar{\phi})$ tout entier. Soit $\bar{V}$ le noyau de $\bar{\phi}$ et V l'image réciproque de $\bar{V}$ dans ϑ_0 (c'est à dire le sous-module engendré par $e_{n+q'+1}, \cdots, e_{n+q}$). La restriction de $\pi^{-1}\phi$ à V est encore une forme à valeurs entières et définit par réduction modulo $\mathfrak{p}$ une forme ϕ' sur $\bar{V}$ qui est anisotrope, donc non dégénérée. Soit d'autre part ϕ'' la forme non dégénérée sur $\bar{E}/\bar{V}$ associée à $\bar{\phi}$. Si $k \in K^0$, alors $\bar{k}$ conserve $\bar{V}$ et par suite définit un automorphisme k'' de $\bar{E}/\bar{V}$ et $k'' \in G(\phi'')$. D'autre part, on vérifie facilement que la restriction k' de $\bar{k}$ à $\bar{V}$ conserve ϕ'. On obtient donc aussi un homomorphisme $k \rightarrow (k', k'')$ de K^0 dans $G(\phi') \times G(\phi'')$ et on déduit facilement de l'étude faite plus haut dans le cas où $\bar{\phi}$ est non dégénérée, que cet homomorphisme est surjectif et envoie N^0 (resp. N'^0) sur le produit $N(\phi') \times N(\phi'')$ (resp. $N'(\phi') \times N'(\phi'')$). On en déduit aussitôt que *tout représentation irréductible de* K^0 *provenant d'une représentation de* $G(\phi') \times G(\phi'')$ *et dont la restriction à* $N^0 \cap K^0$ *contient la représentation unité, satisfait à la condition* (S).

BIBLIOGRAPHIE.

[1] N. Bourbaki, *Algèbre*, Chapitre IX, Paris, 1959.

[2] F. Bruhat, "Distributions sur un groupe localement compact et application à l'étude des représentations des groups $\mathfrak{p}$-adiques," *Bulletin de la Société Mathématique de France*, vol. 89 (1961), p.

[3] ———, "Sur les représentations des groupes classiques $\mathfrak{p}$-adiques," *American Journal of Mathematics*, vol.

[4] J. Dieudonné, *Sur les groupes classiques*, Paris, 1948.

[5] ———, *La géométrie des groupes classiques*, Berlin, 1955.

[6] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Berlin, 1952.

[7] R. Godement, "A theory of spherical functions," *Transactions of the American Mathematical Society*, vol. 73 (1952), pp. 496-556.

[8] H. Hasse, *Zahlentheorie*, Berlin, 1949.

[9] G. W. Mackey, "On induced representations of groups," *American Journal of Mathematics*, vol. 73 (1952), pp. 1145-1162.

SOUS-GROUPES DISCRETS DES GROUPES RESOLUBLES.*

par MASAHIKO SAITO.

Introduction. L'objet de ce mémoire est l'étude de la compacité des espaces quotient des groups de Lie résolubles par des sous-groupes discrets, ainsi que l'étude des structures kählériennes invariantes sur ces groupes en rapport avec la première question. On dira d'après A. I. Malcev qu'un sous-groupe D d'un groupe topologique G est uniforme dans G si l'espace quotient de G par l'adhérence de D est compact. Malcev [3] a démontre que pour qu'il existe un sous-groupe discret et uniforme dans un groupe de Lie nilpotent connexe et simplement connexe G, il faut et il suffit que l'algèbre de Lie $\mathfrak{g}$ de G admette une base par rapport à laquelle les constantes de structure sont toutes rationnelles. Dans ce mémoire, nous établirons un théorème dans une certaine mesure analogue relatif aux groupes de Lie algébriques résolubles.

Dans le § 1, on étudiera diverses questions concernant les sous-groupes discrets des groupes de Lie nilpotents et résolubles.

T. Ono [8] a récemment développé une théorie arithmétique des groupes algébriques; il a notamment généralisé le théorème des unités de Dirichlet aux groupes algébriques résolubles en se servant des caractères rationnels d'un groupe algébrique. D'un autre côté, d'après G. D. Mostow [5], si G est un sous-groupe algébrique irréductible et résoluble de $GL(n, \boldsymbol{Q})$, l'espace quotient du plus petit sous-groupe algébrique de $GL(n, \boldsymbol{R})$ contenant G par $G \cap GL(n, \boldsymbol{Z})$ est revêtu un nombre fini de fois par le produit d'un espace euclidien et d'un espace compact. On déduira sans difficulté des résultats de Ono que la dimension de la partie euclidienne est égale au rang du groupe des caractères rationnels de G (Théorème 2).

Dans le § 3, la question d'existence d'un sous-groupe discret et uniforme dans un groupe de Lie algébrique résoluble sera ramenée à celle de l'uniformité dans un certain groupe matriciel associé du sous-groupe des matrices entières de déterminant ± 1 (Théorème 3). En tenant compte du Théorème 2, on peut dans une certaine mesure exprimer ces conditions au moyen des caractères rationnels du groupe associé (Corollaires 1 et 2).

Dans le § 4, on déterminera d'abord la structure des groupes résolubles algébriques (ou bien des groupes de Lie résolubles connexes et simplement

---

* Received January 17, 1961.

connexes) qui admettent des sous-groupes commutatifs discrets et uniformes (Théorèmes 4 et 5). En tenant compte d'un résultat de J. Hano [2], on saura qu'un tel groupe, pourvu qu'il soit de dimension paire, admet une structure kählérienne invariante (à gauche ou à droite). Si en particulier le groupe est unimodulaire et algébrique, la réciproque est aussi vraie (Théorème 5).

Le reste de ce mémoire est consacré à une construction d'une variété abélienne à partir d'une structure kählérienne invariante sur un groupe de Lie résoluble connexe et simplement connexe. Un résultat partiel de ce paragraphe a déjà été annoncé dans [10].

L'auteur désire exprimer ici sa profonde reconnaissance à Monsieur C. Chevalley pour ses suggestions utiles et son constant encouragement au cours de ce travail. Entre autres choses, la démonstration de la Proposition 5 lui est due.

Notations. On désignera par $\boldsymbol{Z}$, $\boldsymbol{Q}$ et $\boldsymbol{R}$ respectivement l'anneau des entiers rationnels, le corps des nombres rationnels et le corps des nombres réels. Si K est un corps, $GL(n, K)$ et $\mathfrak{gl}(n, K)$ désigneront respectivement le groupe des matrices inversibles de degré n à coefficients dans K et l'algèbre de Lie des matrices de degré n à coefficients dans K. On désignera par $GL(n, \boldsymbol{Z})$ le groups des matrices de déterminant ± 1 de degré n à coefficients dans $\boldsymbol{Z}$. Si G est un sous-groupe de $GL(n, \boldsymbol{R})$ ou de $GL(n, \boldsymbol{Q})$, G^{Q} et G^{Z} seront respectivement $G \cap GL(n, \boldsymbol{Q})$ et $G \cap GL(n, \boldsymbol{Z})$. Si G est un sous-groupe de $GL(n, \boldsymbol{Q})$, G^{R} sera le plus petit sous-groupe algébrique de $GL(n, \boldsymbol{R})$ contenant G.

Si G est un groupe de Lie, Ad et ad désigneront respectivement la représentation adjointe de G et sa différentielle. Pour un groupe G et pour une algèbre de Lie $\mathfrak{g}$, $\mathscr{C}^{i}(G)$ et $\mathscr{C}^{i}(\mathfrak{g})$ désigneront respectivement le i-ième terme de la séries centrale décroissante de G et de $\mathfrak{g}$.

1. Groupes de Lie nilpotents et résolubles.

Définition. Soient G un groupe topologique et D un sous-groupe de G. On dira d'après A. I. Malcev [3] que D est uniforme dans G si l'espace quotient de G par l'adhérence de D dans G est compact.

Le théorème suivant démontré par G. D. Mostow [5] jouera un rôle fondamental dans notre raisonnement.

THÉORÈME M. *Soient G un groupe de Lie résoluble connexe, D un sous-groupe discret et uniforme de G et N le plus grand sous-groupe analytique* *distingué et nilpotent de G. Alors $D \cap N$ est uniforme dans N et par conséquent DN est fermé dans G.*

Définition. Soit $\mathfrak{g}$ une algèbre de Lie sur un corps de caractéristique 0. Une base de $\mathfrak{g}$ sera dite *rationnelle* si les constantes de structure de $\mathfrak{g}$ par rapport à cette base sont toutes rationnelles.

Le théorème de Campbell-Hausdorff-Dynkin (voir [11]) appliqué aux groupes de Lie nilpotents nous donne le lemme suivant.

LEMME 1. *Soient G un groupe de Lie nilpotent et $\mathfrak{g}$ son algèbre de Lie. Supposons qu'il existe une base rationnelle $X_1, \cdots, X_n$ de $\mathfrak{g}$. Alors tout élément du sous-groupe de G engendré par les éléments* $\exp X_i$ $(1 \leqq i \leqq n)$ *peut s'écrire sous la forme* $\exp X$, *où X est une combination linéaire de $X_1, \cdots, X_n$ à coefficients rationnels.*

PROPOSITION 1. *Soient G un groupe de Lie nilpotent connexe et simplement connexe et D un sous-groupe uniforme de G. Alors $\mathscr{C}^i(D)$ est uniforme dans $\mathscr{C}^i(G)$ pour tout i.*

On démontrera la proposition par récurrence sur i. Supposons que $\mathscr{C}^{i-1}(D)$ soit uniforme dans $\mathscr{C}^{i-1}(G)$. Soit H l'intersection de tous les sous-groupes analytiques de G contenant $\mathscr{C}^i(D)$. H est lui-même un sous-groupe analytique et $\mathscr{C}^i(D)$ est uniforme dans H (voir [9]). Désignons par $\mathfrak{g}$, $\mathfrak{h}$ les algèbres de Lie de G, H respectivement. Alors $\mathfrak{h}$ est le sous-espace de $\mathfrak{g}$ engendré par les éléments X de $\mathfrak{g}$ tels que $\exp X \in \mathscr{C}^i(D)$ (voir [9]). Soient x un élément de D et y un élément de $\mathscr{C}^i(D)$. Il existe donce des éléments uniquement détermines X de $\mathfrak{g}$ et Y de $\mathfrak{h}$ tels que $x = \exp X$ et $y = \exp Y$. Puisque $\exp Adx(Y) = xyx^{-1} \in \mathscr{C}^i(D) \subset H$, $Adx(Y)$ appartient à $\mathfrak{h}$. Comme Adx est un endomorphisme unipotent, adX peut s'écrire sous la forme d'un polynôme de Adx. Donc l'élément $[X, Y] = adX(Y)$ appartient à $\mathfrak{h}$. Puisque les éléments X engendrent $\mathfrak{g}$ (voir [9]), $\mathfrak{h}$ est un idéal de $\mathfrak{g}$.

Soient maintenant x un élément de D et y un élément de $\mathscr{C}^{i-1}(D)$. Posons $x = \exp X$, $y = \exp Y$ où $X \in \mathfrak{g}$ et $Y \in \mathscr{C}^{i-1}(\mathfrak{g})$. On a la relation de congruence $xyx^{-1} \equiv y (\operatorname{mod} H)$, d'où la relation $Adx(Y) \equiv Y (\operatorname{mod} \mathfrak{h})$. En passant à l'égalité dans l'algèbre quotient $\mathfrak{g}/\mathfrak{h}$, on peut conclure par le même raisonnement que le précédent que l'élément $[X, Y]$ appartient à $\mathfrak{h}$. Donc on a $\mathscr{C}^i(\mathfrak{g}) = [\mathfrak{g}, \mathscr{C}^{i-1}(\mathfrak{g})] \subset \mathfrak{h}$. L'inclusion au sens inverse étant évidente, on a $\mathscr{C}^i(\mathfrak{g}) = \mathfrak{h}$, ce qui achève la démonstration de la Proposition 1.

Soit D un groupe résoluble. On dira qu'un ensemble ordonné $\{x_1, \cdots, x_n\}$ d'éléments de D est un *système libre de générateurs* si tout élément de D peut se représenter dans une seule façon sous la forme $\prod_{i=1}^{n} x_i^{a_i}$, où des a_i sont des entiers.

Soit $\mathfrak{g}$ une algèbre de Lie et soit $\mathfrak{g}_0, \mathfrak{g}_1, \cdots, \mathfrak{g}_r$ une série nomale de $\mathfrak{g}$; c'est-à-dire, une série décroissante de sous-algèbres telle que $\mathfrak{g}_0 = \mathfrak{g}$, $\mathfrak{g}_r = \{0\}$ et que $\mathfrak{g}_i$ soit un idéal dans $\mathfrak{g}_{i-1}$ $(1 \leqq i \leqq r)$. Une base $X_1, \cdots, X_n$ de $\mathfrak{g}$ sera dite *adaptée* à cette série si, pour pour tout i, il existe une partie de cette base qui forme une base de $\mathfrak{g}_i$.

La proposition suivante est due à Y. Matsushima (voir [4] Theorem 3).

PROPOSITION 2. *Soient G un groupe de Lie nilpotent connexe et simplement connexe et D un sous-groupe discret et uniforme dans G. Il existe alors une base $X_1, \cdots, X_n$ de l'algèbre de Lie $\mathfrak{g}$ de G adaptée à la série centrale décroissante de $\mathfrak{g}$ telle que, si l'on pose $x_i = \exp X_i$, les éléments $x_1, \cdots, x_n$ constituent un système libre de générateurs de D.*

PROPOSITION 3. *Les notations étant celles de la Proposition 2, la base $X_1, \cdots, X_n$ de $\mathfrak{g}$ est rationnelle.*

Soit en effet $\mathfrak{g}_i$ $(1 \leqq i \leqq n)$ le sous-espace de $\mathfrak{g}$ engendré par les éléments $X_{i+1}, \cdots, X_n$. Les $\mathfrak{g}_i$ sont des sous-algèbres de $\mathfrak{g}$. Démontrons par récurrence sur i que les éléments $X_{i+1}, \cdots, X_n$ constituent une base rationnelle de $\mathfrak{g}_i$. L'assertion est triviale pour $i = n$. Supposons qu'elle soit vraie pour les indices supérieurs à i. Soit k un nombre plus grand que i. Puisque notre base s'adapte à la série centrale décroissante de $\mathfrak{g}$, l'élément $x_i x_k x_i^{-1}$ est de la forme $\prod_{j=k+1}^{n} x_j^{a_j}$, les a_j étant entiers. Par l'hypothèse de récurrence, les éléments $X_{k+1}, \cdots, X_n$ forment une base rationnelle de $\mathfrak{g}_k$. Par le Lemme 1, l'élément $\prod_{j=k+1}^{n} x_j^{a_j}$ est de la forme $\exp(\sum_{j=k+1}^{n} b_j X_j)$, où les b_j sont des nombres rationnels. Utilisant l'égalité $x_i x_k x_i^{-1} = \exp Ad x_i(X_k)$, on obtient la relation $Ad x_i(X_k) = \sum b_j X_j$. $Ad x_i$ étant unipotent, $ad X_i$ peut s'écrire sous la forme d'un polynôme à coefficients rationnels de $Ad x_i$. On obtient donc $[X_i, X_k] = \sum_{j=k+1}^{n} c_j X_j$, où les c_j sont des nombres rationnels, ce qui démontre la Proposition 3.

THÉORÈME 1. *Soient G un groupe de Lie résoluble connexe et simplement connexe, N le plus grand sous-groupe analytique distingué nilpotent de G et D un sous-groupe discret uniforme de G. Il existe alors un système libre de générateurs $x_1, \cdots, x_n$ de D dont une partie $x_{r+1}, \cdots, x_n$ forme un système libre de générateurs de $D \cap N$ tel que, si l'on pose $x_i = \exp X_i$ $(r+1 \leqq i \leqq n)$, les éléments $X_{r+1}, \cdots, X_n$ constituent une base rationnelle de l'algèbre de Lie $\mathfrak{n}$ de N adaptée à la serié centrale décroissante de $\mathfrak{n}$.*

Par le Théorème M, $D \cap N$ et DN/N sont sous-groupes discrets et uniformes dans N et G/N respectivement. It existe donc par les Propositions 2 et 3 une base rationnelle $X_{r+1},\cdots,X_n$ de $\mathfrak{n}$ adaptée à la série centrale décroissante de $\mathfrak{n}$ telle que, si l'on pose $x_i=\exp X_i$ $(r+1\leqq i\leqq n)$, les éléments $x_{r+1},\cdots,x_n$ forment un système libre de générateurs de $D\cap N$. D'un autre côté, il existe un système libre de générateurs $x_1^*,\cdots,x_r^*$ de DN/N. Prenons une image réciproque x_i de x_i^* dans D $(1\leqq i\leqq r)$. Alors les éléments $x_1,\cdots,x_n$ forment un système libre de générateurs de D ayant les propriétés voulues, ce qui démontre le Théorème 1.

PROPOSITION 4. *Soient G un groupe de Lie résoluble connexe et simplement connexe et D un sous-groupe discret et uniforme de G. Désignons par $l(G)$ èt $l(D)$ les longeurs des séries des commutateurs de G et de D repectivement. Alors*

$$l(G)\geqq l(D)\geqq l(G)-1.$$

Si G est nilpotent, l'égalité $l(G)=l(D)$ a lieu.

Soit d'abord G nilpotent. Supposons que la dernière égalité ait lieu pour les groupes nilpotents de longueurs moins que celle de G. $[D,D]$ est uniforme dans $[G,G]$ par la Proposition 1. Par l'hypothèse de récurrence, on a l'égalité $l([G,G])=l([D,D])$, d'où l'égalité $l(G)=l(D)$. Dans le cas général, soit N le plus grand sous-groupe analytique distingué nilpotent de G. Le Théorème M dit que $D\cap N$ est uniforme dans N et donc que $l(D\cap N)=l(N)$. Puisque N contient le groupe des commutateurs $[G,G]$ de G, on a $l(G)-1\leqq l(N)=l(D\cap N)\leqq l(D)$, ce que démontre la Proposition 4.

G. D. Mostow [7] a introduit la notion de rang d'un groupe résoluble. Soit D un groupe résoluble et soit $\mathfrak{D}^i(D)$ le i-ième terme de sa série des commutateurs. Le *rang* de D est défini par la somme suivante:

$$\operatorname{rang} D=\sum_i \operatorname{rang}(\mathfrak{D}^{i-1}(D)/\mathfrak{D}^i(D))$$

Les rangs du côté droit sont des rangs dans le sens usuel des groupes commutatifs. Puisque D est résoluble, la sommation est finie. Nous énumérons ci-dessous quelques propriétés du rang d'un groupe résoluble (voir [7] et [8]).

1. Si D' est un sous-groupe d'un groupe résoluble D, on a alors $\operatorname{rang} D'\leqq\operatorname{rang} D$. Si en particulier D' est d'indice fini dans D, on a l'égalité $\operatorname{rang} D'=\operatorname{rang} D$.

2. Si D' est un sous-groupe distingué de D, alors $\operatorname{rang} D=\operatorname{rang} D/D'$

$+\operatorname{rang} D'$. Donc, pour n'importe quelle série normale $D_0, D_1, \cdots, D_r$ de D, on a

$$\operatorname{rang} D = \sum_{i=1}^{r} \operatorname{rang} D_{i-1}/D_i.$$

3. Soient G un groupe de Lie résoluble connexe et simplement connexe et D un sous-groupe discret de G. Alors $\operatorname{rang} D \leqq \dim G$.

4. Si un group résoluble D admet un système libre de générateurs $x_1, \cdots, x_n$, alors le nombre n est égal à rang D.

Soit G un groupe de Lie à un nombre fini de composantes connexes. Il existe alors d'après [6] un sous-groupe compact maximal de G, et deux sous-groupes compacts maximaux de G sont conjugués par un automorphisme intérieur de G.

LEMME 2. *Soient G un groupe de Lie résoluble à un nombre fini de composantes connexes, K un sous-groupe compact maximal de G et D un sous-groupe discret de G. Alors* $\operatorname{rang} D$ *est fini et au plus égal à* $\dim G - \dim K$. *Supposons qu'il existe un sous-groupe analytique fermé distingué et nilpotent N tel que le groupe quotient G/N soit nilpotent et que le sous-groupe DN soit fermé. Alors pour que l'égalité* $\operatorname{rang} D = \dim G - \dim K$ *ait lieu, il faut et il suffit que D soit uniforme dans G.*

Soit G_0 la composante connexe de l'élément neutre de G. Alors $D \cap G_0$ est d'indice fini dans D, et par suite $\operatorname{rang} D = \operatorname{rang} D \cap G_0$. D'un autre côté, G/D est compact si et seulement si $G_0/D \cap G_0$ est compact. On peut donc supposer G connexe.

Soient $\tilde{G}$ le revêtement universel de G et $\tilde{D}$ l'images réciproque de D dans $\tilde{G}$. Alors $\operatorname{rang} \tilde{D}$ est fini et au plus égal à $\dim \tilde{G}$ par la troisième propriété du rang. Soit A le noyau de l'homomorphisme canonique de $\tilde{G}$ sur G. La deuxième propriété du rang entraîne l'égalité $\operatorname{rang} \tilde{D} - \operatorname{rang} D = \operatorname{rang} A$. Soit encore $\tilde{K}$ la composante connexe de l'élément neutre de l'image réciproque de K dans $\tilde{G}$. Puisque $\tilde{K}$ est le revêtement universel du tore K et que l'espace quotient G/K est simplement connexe, A est contenu dans $\tilde{K}$ et donc $\operatorname{rang} A = \dim K$. On a donc l'inégalité $\operatorname{rang} D \leqq \dim G - \dim K$, ce qui démontre la première assertion. Il suffira de démontrer la deuxième assertion pour le cas simplement connexe.

Supposons G nilpotent. L'assertion est évidemment vraie pour les groupes commutatifs. Supposons qu'elle soit vraie pour les groupes dont la longueur de la série centrale décrossante est moindre que celle de G. Si D est uniforme dans G, $D \cap \mathscr{C}^1(G)$ est uniforme dans $\mathscr{C}^1(G)$ par la Proposition 1 et par suite $D\mathscr{C}^1(G)$ est fermé. Donc les sous-groupes discrets $D\mathscr{C}^1(G)/\mathscr{C}^1(G)$ et $D \cap \mathscr{C}^1(G)$ sont respectivement uniformes dans $G/\mathscr{C}^1(G)$ et $\mathscr{C}^1(G)$. L'hypothèse de récurrrence entraîne les deux égalités $\operatorname{rang}(D\mathscr{C}^1(G)/\mathscr{C}^1(G)) = \dim(G/\mathscr{C}^1(G))$ et $\operatorname{rang}(D\mathscr{C}^1(G)) = \dim \mathscr{C}^1(G)$; d'où l'égalité voulue $\operatorname{rang} D = \dim G$.

Supposons réciproquement $\operatorname{rang} D = \dim G$. Soit H le plus petit sous-groupe analytique de G contenant D. D est uniforme dans H; mais H est égal à G par l'inégalité $\operatorname{rang} D \leqq \dim H$, ce qui démontre notre assertion.

Considérons le cas général. Par l'hypothèse, DN/N et $D \cap N$ sont des sous-groupes discrets dans G/N et N respectivement. Donc on a les inégalités $\operatorname{rang} DN/N \leqq \dim G/N$ et $\operatorname{rang} D \cap N \leqq \dim N$. Si D est uniforme dans G, DN/N et $D \cap N$ sont uniformes dans G/N et N. Puisque G/N et N sont nilpotents, on a les deux égalités $\operatorname{rang} DN/N = \dim G/N$ et $\operatorname{rang} D \cap N = \dim N$, qui entraînent l'égalité voulue. Si réciproquement l'égalité $\operatorname{rang} D = \dim G$ a lieu, on obtient, en vertu des deux inégalités ci-dessus, les deux égalités $\operatorname{rang} DN/N = \dim G/N$ et $\operatorname{rang} D \cap N = \dim N$. Donc DN/N et $D \cap N$ sont uniformes dans G/N et N respectivement, puisque G/N et N sont nilpotents. Ceci implique que D est uniforme dans G. Le Lemme 2 est donc démontré.

2. Groupes algébriques résolubles. Soit K un corps de caractéristique 0. On entendra par K-tore un sous-groupe algébrique irréductible et commutatif de $GL(n, K)$ formé de matrices semi-simples.

Soient G un sous-groupe algébrique irréductible et résoluble dans $GL(n, K)$, G_u le sous-groupe des matrices unipotentes de G et S un K-tore maximal contenu dans G. Alors G se décompose en produit semi-direct de S et de G_u, G_u étant distingué dans G. Si on désigne par $\mathfrak{g}$, $\mathfrak{g}_u$ et $\mathfrak{s}$ respectivement les algèbres de Lie de G, de G_u et de S, on obtient une décomposition de $\mathfrak{g}$ en produit semi-direct de $\mathfrak{s}$ et de $\mathfrak{g}_u$. On appellera ces décompositions *décomposition de Chevalley.*

LEMME 3. *Soit K un corps de caractéristique* 0. *Soit $\mathfrak{g}$ une sous-algèbre algébrique commutative de $\mathfrak{gl}(n, K)$ composée de matrices semi-simples. Alors, si $\mathfrak{g} \neq \{0\}$, il existe un élément A de $\mathfrak{g}$ ted que* $\operatorname{Tr} A^2 \neq 0$.

Soit $\bar{K}$ une extension algébriquement close de K, et soit $\bar{\mathfrak{g}}$ la sous-algèbre de $\mathfrak{gl}(n, \bar{K})$ engendrée par $\mathfrak{g}$. On peut transformer simultanément les matrices de $\bar{\mathfrak{g}}$ en matrices diagonales; supposons que $X \in \bar{\mathfrak{g}}$ soit transformé en

$(\alpha_1(X),\cdots,\alpha_n(X))$. Alors les matrices de $\bar{\mathfrak{g}}$ sont caractérisées par un certain nombre de relations linéaires à coefficients rationnels entre les $\alpha_i(X)$, qui peuvent se mettre sous la forme $\alpha_{m+i}(X)=\sum_{j=1}^{m}c_{ij}\alpha_j(X)$ $(1\leqq i\leqq n-m)$, les c_{ij} étant rationnels. La forme quadratique $\sum_{j=1}^{m}X_j^2+\sum_{i=1}^{n-m}(\sum_{j=1}^{m}c_{ij}X_j)^2$ étant >0, il existe un élément $X\in\bar{\mathfrak{g}}$ tel que $\mathrm{Tr}\,X^2\neq 0$. Si $A_1,\cdots,A_r$ est une base de $\mathfrak{g}$, la forme quadratique $\sum_{i,j}c_{ij}\,\mathrm{Tr}\,A_iA_j$ qui prend des valeurs $\neq 0$ sur $\bar{K}$ prend aussi des valeurs $\neq 0$ sur K. Le Lemme 3 est donc démontré.

COROLLAIRE. *La forme bilinéaire* $(A,B)\to\mathrm{Tr}\,AB$ *sur* $\mathfrak{g}\times\mathfrak{g}$ *est non-dégénérée.*

En effet, utilisons les notations de la démonstration précédente. Soit S une matrice de $GL(n,\bar{K})$ telle que $S\mathfrak{g}S^{-1}$ soit composé de matrices diagonales; alors les matrices $\bar{Y}$ telles que $S\bar{Y}S^{-1}$ soient diagonaux et que $\mathrm{Tr}\,\bar{X}\bar{Y}=0$ pour tout $\bar{X}\in\mathfrak{g}$ forment une algèbre de Lie algébrique $\bar{\mathfrak{h}}$, donc $\bar{\mathfrak{g}}\cap\bar{\mathfrak{h}}$ est algébrique, d'où $\mathfrak{g}\cap\mathfrak{h}=\{0\}$ d'après le résultat précédent. On a donc démontré le Corollaire.

PROPOSITION 5. *Soit* K *un corps de caractéristique* 0, *et soit* $\mathfrak{g}$ *une sous-algèbre algébrique commutative de* $\mathfrak{gl}(n,K)$. *Alors* $\mathfrak{g}$ *se décompose en produit direct de sous-algèbres algébriques qui n'admettent aucune sous-algèbre algébrique.*

En effet, soit $\mathfrak{g}=\mathfrak{g}_s\times\mathfrak{g}_u$ la décomposition de Chevalley de $\mathfrak{g}$. Puisque toute algèbre formée de matrices nilpotentes est algébrique, $\mathfrak{g}_u$ est le produit direct de sous-algèbres algébriques de dimension 1. De l'autre côté, supposons que $\mathfrak{g}_s$ admette une sous-algèbre algébrique $\mathfrak{a}$. Soit $\mathfrak{b}$ le sous-espace de $\mathfrak{g}_s$ formé des matrices X de $\mathfrak{g}_s$ telles que $\mathrm{Tr}\,XY=0$ pour tout $Y\in\mathfrak{a}$. D'après le Corollaire précédent, $\mathfrak{b}$ est une algèbre de Lie algébrique et $\mathfrak{g}_s$ se décompose en produit direct de $\mathfrak{a}$ et de $\mathfrak{b}$, ce qui achève la démonstration de la Proposition 5.

LEMME 4. *Soit* $\mathfrak{g}$ *une sous-algèbre algébrique commutative de* $\mathfrak{gl}(n,\boldsymbol{R})$ *formée de matices semi-simples. Alors* $\mathfrak{g}$ *est le produit direct de la sous-algèbre algébrique des matrices à valeurs propres réelles et de la sous-algèbre algébrique des matrices à valeurs propres purement imaginaires.*

On peut supposer que tout élément X de $\mathfrak{g}$ est de la forme:

$$\begin{pmatrix} \boxed{\begin{matrix} a_1 & -b_1 \\ b_1 & a_1 \end{matrix}} & & & & & \\ & \ddots & & & & \\ & & \boxed{\begin{matrix} a_r & -b_r \\ b_r & a_r \end{matrix}} & & & \\ & & & c_1 & & \\ & & & & \ddots & \\ & & & & & c_s \end{pmatrix}.$$

Alors la partie diagonale Y de X et la matrice $X-Y$ sont des répliques de X, donc appartiennent à $\mathfrak{g}$. L'expression $X=Y+(X-Y)$ donne la décomposition de $\mathfrak{g}$.

COROLLAIRE. *Soit G un $\mathbf{R}$-tore. Alors G est engendré par le plus grand sous-groupe compact de G et par le plus grand sous-groupe algébrique irréductible diagonalisable de G. Leur intersection est finie.*

C'est une conséquence directe du Lemme 4.

Définition. Soit G un groupe algébrique de matrices à coefficients dans un corps K. Un *caractère rationnel* de G est une représentation rationnelle de G dans le groupe multiplicatif des éléments non-nuls de K. On définit la multiplication de deux caractères rationnels χ, χ' par la formule

$$(\chi\chi')(x)=\chi(x)\chi'(x) \quad \text{pour } x\in G.$$

Alors l'ensemble de tous les caractères rationnels de G forme un groupe commutatif, qu'on désignera par $\mathrm{X}(G)$.

PROPOSITION 6. *Soient G un $\mathbf{R}$-tore et K le plus grand sous-groupe compact de G. Alors le groupe des caractères rationnels $\mathrm{X}(G)$ de G est un groupe commutatif sans torsion de rang égal à* $\dim G-\dim K$.

Les Propositions 1 et 2 de T. Ono [8] disent que $\mathrm{X}(G)$ est un groupe commutatif sans torsion de rang fini. Soit H le plus grand sous-groupe algébrique irréductible diagonalisable de G. Alors la restriction d'un charactère rationnel de G à H est un homomorphisme de $\mathrm{X}(G)$ dans $\mathrm{X}(H)$. D'après le Corollaire du Lemme 4, cet homomorphisme est de noyau fini et de conoyau fini. Le rang de $X(G)$ est donc égal au rang de $X(H)$. H étant diagonalisable, rang $X(H) = \dim H$, ce qui démontre la Proposition 6.

Soit G un sous-groupe algébrique irréductible résoluble de $GL(n, \boldsymbol{Q})$. D'après G. D. Mostow [5], avec un peu de modification, l'espace quotient G^{R}/G^{Z} est revêtu un nombre fini de fois par le produit direct d'un espace euclidien et d'un espace compact. Il n'est pas difficile de voir que la dimension de la partie euclidienne de G^{R}/G^{Z}, désignée par $\nu(G^{R}/G^{Z})$, est égale à $\dim G^{R} - \dim K - \mathrm{rang}\, G^{Z}$ où K est un sous-groupe compact maximal de G^{R}.

Théorème 2. *Les notations étant comme ci-dessus, on a l'égalité*

$$(G^{R}/G^{Z}) = \mathrm{rang}\, X(G).$$

Soient en effet G_u le sous-groupe de G formé des matrices unipotentes de G et S un $\boldsymbol{Q}$-tore maximal contenu dans G. Alors $G = S \cdot G_u$ et $G^{R} = S^{R} \cdot G_u{}^{R}$ sont des décompositions de Chevalley pour G et G^{R} respectivement. La projection de G sur S est une représentation polynômiale (voir la démonstration de la Proposition 15 de T. Ono [8]) ; le groupe $S^{Z} \cdot G_u{}^{Z}$ est donc d'indice fini dans G^{Z} par la Proposition 13(δ) de Ono [8]. On a toujours l'égalité $\dim G_u = \mathrm{rang}\, G_u{}^{Z}$ (voir Proposition 18, Ono [8]) et le théorème des unités pour les $\boldsymbol{Q}$-tores (voir [8]) dit que

$$\mathrm{rang}\, G^{Z} = \mathrm{rang}\, X(G^{R}) - \mathrm{rang}\, X(G).$$

En combinant ces égalités, on obtient l'égalité voulue.

Corollaire. *Les notations étants comme ci-dessus, pour que G^{Z} soit uniforme dans G^{R}, il faut et il suffit que G n'admette pas de caractère rationnel non-trivial.*

Ce Corollaire est aussi une conséquence directe du fait qu'un groupe algébrique irréductible résoluble est de type (C) dans le sens de Ono [8]. Il est donc un cas spécial d'un théorème plus général.

3. Sous-groupes discrets de groupes résolubles.

Lemme 5. *Soient G un sous-groupe algébrique de $GL(m, \mathfrak{R})$ et f une représentation rationnelle de G dans $GL(n, \boldsymbol{R})$, m et n étant des entiers positifs. Alors l'image $f(G)$ est d'indice fini dans son adhérence algébrique dans $GL(n, \boldsymbol{R})$, et donc fermée dans $GL(n, \boldsymbol{R})$.*

En effet, la composante connexe G_0 de l'élément neutre de G est d'indice fini dans G (voir [7]). Soient N le noyau de f et G^{*} l'adhérence algébrique de $f(G)$ dans $GL(n, \boldsymbol{R})$. Alors $\dim G^{*} = \dim G - \dim N$. D'un autre côté,

$\dim f(G_0) = \dim G - \dim N$. Par conséquent $f(G_0)$ est la composante connexe de l'élément neutre dans G^*, et donc d'indice fini dans G^*, ce qui finit la démonstration du Lemme 5.

La Proposition 6, § 5, Ch. V de Chevalley [1] nous donne le lemme suivant.

LEMME 6. *Soient* $\mathfrak{g}$ *une algèbre de Lie résoluble sur un corps de caractéristique* 0 *et* $\mathfrak{n}$ *le plus grand idéal nilpotent de* $\mathfrak{g}$. *Supposons que l'image de* $\mathfrak{g}$ *par sa représentation adjointe soit algébrique. Il existe alors dans* $\mathfrak{g}$ *une sous-algèbre commutative* $\mathfrak{a}$ *telle que* $\mathfrak{g}$ *se décompose en produit semi-direct de* $\mathfrak{a}$ *et de* $\mathfrak{n}$.

Le lemme suivant est bien connu.

LEMME 7. *Soit* G *un groupe commutatif d'automorphismes semi-simples d'un espace vectoriel* V *de dimension finie sur un corps. Supposons que* G *laisse stable un sous-espace* U *de* V. *Alors la représentation identique de* G *est équivalente à la somme directe des représentations sur* U *et sur* V/U *qui se déduisent de la représentation identique.*

Soit G un groupe. Deux sous-groupes D et D' de G seront dits *commensurables* si leur intersection $D \cap D'$ est d'indice fini dans chacun d'eux. Le lemme suivant est bien connu (on peut en trouver une démonstration dans l'introduction de A. Weil ([12]).

LEMME 8. *Soient* G *et* H *des sous-groupes algébriques de* $GL(m, \boldsymbol{Q})$ *et* $GL(n, \boldsymbol{Q})$ *respectivement. Supposons qu'il existe un isomorphisme rationnel* f *de* G *sur* H. *Alors* $H^{\mathbf{Z}}$ *et* $f(G^{\mathbf{Z}})$ *sont commensurables.*

LEMME 9. *Soient* G *un groupe de Lie nilpotent connexe et* Z *son centre. Désignons par* $\mathfrak{g}$, $\mathfrak{z}$ *les algèbres de Lie de* G, Z *respectivement. Soient* $\mathfrak{m}$ *un sous-espace complémentaire de* $\mathfrak{z}$ *dans* $\mathfrak{g}$ *et* M *le sous-ensemble de* G *formé des éléments de la forme* $\exp X$, *où* $X \in \mathfrak{m}$. *Alors tout élément de* G *se représente dans une seule façon comme le produit d'un élément de* M *et d'un élément de* Z.

Soit en effet x un élément de G. Il existe un élément X de $\mathfrak{g}$ tel que $x = \exp X$. X est la somme d'un élément $X_{\mathfrak{m}}$ de $\mathfrak{m}$ et d'un élément $X_{\mathfrak{z}}$ de $\mathfrak{z}$. Si l'on pose $x_{\mathfrak{m}} = \exp X_{\mathfrak{m}}$ et $x_{\mathfrak{z}} = \exp X_{\mathfrak{z}}$, on obtient une décomposition voulue: $x = x_{\mathfrak{m}} \cdot x_{\mathfrak{z}}$.

Supposons ensuite qu'il y ait deux décompositions $x = x_{\mathfrak{m}} \cdot x_{\mathfrak{z}} = y_{\mathfrak{m}} \cdot y_{\mathfrak{z}}$ où $x_{\mathfrak{m}}, y_{\mathfrak{m}} \in M$, $x_{\mathfrak{z}}, y_{\mathfrak{z}} \in Z$. On a $x_{\mathfrak{m}} = y_{\mathfrak{m}}(y_{\mathfrak{z}} x_{\mathfrak{z}}^{-1})$. On peut donc supposer qu'un élément x de M est de la forme $x_\mathfrak{m} \cdot x_\mathfrak{z}$, où $x_\mathfrak{m} \in W$ et $x_\mathfrak{z} \in Z$. Supposons momentanément G simplement connexe. Il existe alors des éléments uniquement déterminés X, $X_\mathfrak{m}$ de $\mathfrak{m}$ et $X_\mathfrak{z}$ de $\mathfrak{z}$ tels que $x = \exp X$, $x_\mathfrak{m} = \exp X_\mathfrak{m}$ et $x_\mathfrak{z} = \exp X_\mathfrak{z}$. (Il est à remarquer que Z est connexe). On a $X = X_\mathfrak{m} + X_\mathfrak{z}$, d'où $X = X_\mathfrak{m}$, $X_\mathfrak{z} = 0$. Donc notre assertion est vraie si G est simplement connexe. Soit maintenant $\tilde{G}$ le revêtement universel de G, et soient $\tilde{x}$, $\tilde{x}_\mathfrak{m}$, $\tilde{x}_\mathfrak{z}$ respectivement les éléments des images réciproques de x, $x_\mathfrak{m}$, $x_\mathfrak{z}$ dans $\tilde{G}$. On a alors $\tilde{x} = \tilde{x}_\mathfrak{m} \cdot \tilde{x}_\mathfrak{z} \cdot \tilde{y}$, où $\tilde{y}$ est un élément du centre de $\tilde{G}$. Donc $\tilde{x} = \tilde{x}_\mathfrak{m}$, ce qui entraîne les relations $x = x_\mathfrak{m}$ et $x_\mathfrak{z} = e$. Le Lemme 9 est donc démontre.

Soit G un groupe de Lie résoluble. Dans tout ce qui suit, P désignera la représentation de G sur le plus grand idéal nilpotent de l'algèbre de Lie de G qui se déduit de la représentation adjointe de G. Désignons par ρ la différentielle de P.

THÉORÈME 3. *Soit G un groupe algébrique résoluble d'automorphismes d'un espace vectoriel de dimension finie sur le corps des nombres réels. Alors pour qu'il existe dans G un sous-groupe discret et uniforme, il faut et il suffit que le plus grand idéal nilpotent $\mathfrak{n}$ de l'algèbre de Lie $\mathfrak{g}$ de G admette une base rationnelle $\mathfrak{B}$ telle que les deux conditions suivantes soient satisfaites.*

1) *Soit N le sous-groupe analytique de G correspondant à $\mathfrak{n}$, et soient K et $\mathfrak{k}$ le plus grand sous-groupe compact de N et son algèbre de Lie. Alors la base $\mathfrak{B}$ est adaptée à la série normale $\mathfrak{n}$, $\mathfrak{k}$, $\{0\}$ de $\mathfrak{n}$.*

2) *Si on considère $\mathrm{P}(G)$ comme un groupe de matrices par rapport à $\mathfrak{B}$, $\mathrm{P}(G)^{\mathbf{Z}}$ est uniforme dans $\mathrm{P}(G)$.*

THÉORÈME 3′. *Soit G un groupe de Lie résoluble à un nombre fini de composantes connexes. Supposons que l'image de l'algèbre de Lie $\mathfrak{g}$ de G par sa représentation adjointe soit algébrique. Alors la conclusion du Théorème 2 est aussi valable pour G.*

Le Théorème 3 est contenu dans le Théorème 3′ en vertu du Lemme 5. On peut supposer sans restreindre la généralité que G est connexe. La démonstration procédera en plusieurs étapes.

1°) Supposons d'abord qu'il existe dans G un sous-groupe discret et uniforme D. Soient $\tilde{G}$ le revêtement universel de G, D l'image réciproque de D dans $\tilde{G}$ et $\tilde{N}$ le plus grand sous-groupe analytique distingué et nilpotent de $\tilde{G}$. Alors $\bar{D} \cap \tilde{N}$ est uniforme dans $\tilde{N}$ par le Théorème M. En vertu du Théorème 1, il existe un système libre de générateurs $u_1, \cdots, u_r$, $x_1, \cdots, x_n$ de $\bar{D}$ dont la partie $x_1, \cdots, x_n$ forme un système libre de générateurs de

$D \cap \tilde{N}$ tel que, si l'on pose $x_i = \exp X_i$ $(1 \leqq i \leqq n)$, les éléments $X_1, \cdots, X_n$ constituent une base rationnelle $\mathfrak{B}'$ de l'algèbre de Lie $\mathfrak{n}$ de $\tilde{N}$ adaptée à la série centrale décroissante de $\mathfrak{n}$. On considérera désormais tout endomorphisme de l'espace vectoriel $\mathfrak{n}$ comme une matrice par rapport à $\mathfrak{B}'$.

2°) On a la relation $\exp Adu_i(X_j) = u_i x_j u_i^{-1} = \prod_{k=1}^{n} x_k^{a_{ijk}}$, où les a_{ijk} sont des entiers. Puisque N est nilpotent et simplement connexe, $Adu_i(X_j)$ est une combinaison linéaire de $X_1, \cdots, X_n$ à coefficients rationnels par le Lemme 1. Les martices $\mathrm{P}u_i$ $(1 \leqq i \leqq r)$ sont donc des matrices rationnelles. Par suite $\mathrm{P}(D)$ est contenu dans $GL(n, \boldsymbol{Q})$ et $\mathrm{P}(G)^{\boldsymbol{Q}}$ est uniforme dans $\mathrm{P}(G)$.

3°) Soit H la composante irréductible de l'élément neutre de l'adhérence algébrique de $\mathrm{P}(G)^{\boldsymbol{Q}}$ dans $GL(n, \boldsymbol{Q})$. $H^{\boldsymbol{R}}$ désigne comme d'habitude l'adhérence algébrique de H dans $GL(n, \boldsymbol{R})$. Alors $\mathrm{P}(G) \cap H^{\boldsymbol{R}}$ est uniforme dans $\mathrm{P}(G)$. D'un autre côté, $H^{\boldsymbol{R}}$ est contenu dans l'adhérence algébrique de $\mathrm{P}(G)$ dans $GL(n, \boldsymbol{R})$ dans laquelle $\mathrm{P}(G)$ est d'indice fini. Donc $\mathrm{P}(G) \cap H^{\boldsymbol{R}}$ est d'indice fini dans $H^{\boldsymbol{R}}$. Puisque $\mathrm{P}(G)^{\boldsymbol{Q}}$ et H sont commensurables, $\mathrm{P}(G)^{\boldsymbol{Z}}$ et $H^{\boldsymbol{Z}}$ le sont aussi. Par conséquent, si on démontre que $H^{\boldsymbol{Z}}$ est uniforme dans $H^{\boldsymbol{R}}$, $\mathrm{P}(G)^{\boldsymbol{Z}} \cap H^{\boldsymbol{Z}}$ sera uniforme dans $\mathrm{P}(G) \cap H^{\boldsymbol{R}}$, et donce $\mathrm{P}(G)^{\boldsymbol{Z}}$ sera uniforme dans $\mathrm{P}(G)$. Il suffit donc de démontrer que $H^{\boldsymbol{Z}}$ est uniforme dans $H^{\boldsymbol{R}}$. Soit S un $\boldsymbol{Q}$-tore maximal contenu dans H. Alors il suffit de démontrer que $S^{\boldsymbol{Z}}$ est uniforme dans $S^{\boldsymbol{R}}$.

4°) Soient P_i les représentations de $\tilde{G}$ sur les espaces $\mathscr{C}^{i-1}(\mathfrak{n})/\mathscr{C}^{i}(\mathfrak{n})$ $(1 \leqq i \leqq s)$ déduites de la représentation P, et soit P_0 la représentation somme-directe de $\mathrm{P}_1, \cdots, \mathrm{P}_s$. Pour un élément x de G, on a:

$$\mathrm{P}(x) = \begin{pmatrix} \boxed{\mathrm{P}_1(x)} & & 0 \\ & \ddots & \\ * & & \boxed{\mathrm{P}_s(x)} \end{pmatrix}, \qquad \mathrm{P}_0(x) = \begin{pmatrix} \boxed{\mathrm{P}_1(x)} & & 0 \\ & \ddots & \\ 0 & & \boxed{\mathrm{P}_s(x)} \end{pmatrix}.$$

Supposons que les éléments $X_{\alpha(i)+1}, \cdots, X_n$ forment une base de $\mathscr{C}^{i}(\mathfrak{n})$, où $0 = \alpha(0) < \cdots < \alpha(s) = n$. Si $\alpha(i-1) < j \leqq \alpha(i)$ et si u est un élément de $\tilde{D}$, on a la relation de congruence

$$u x_j u^{-1} \equiv \prod_{k=\alpha(i-1)+1}^{k=\alpha(i)} x_k^{a_k} \mod \mathscr{C}^{i}(\tilde{N}).$$

Puisque le groupe $\mathscr{C}^{i-1}(\tilde{N})/\mathscr{C}^{i}(\tilde{N})$ est commutatif, on obtient la relation

$$\mathrm{P}_i u(X_j) = \sum_{k=\alpha(i-1)+1}^{k=\alpha(i)} a_k X_k,$$

où les a_k sont des entiers. Donc $\mathrm{P}_i u$ est une matrice entière de déterminant ± 1, de sorte que tout élément de $\mathrm{P}_0(D)$ est une telle matrice. $\mathrm{P}_0(G)^{Z}$ est donc uniforme dans $\mathrm{P}_0(G)$.

5°) La représentation P_0 se factorise comme $\mathrm{P}_0 = \Phi \circ \mathrm{P}$, où Φ est une représentation de $\mathrm{P}(G)$. Φ donne par la manière naturelle une représentation de H^{R}, laquelle nous désignerons encore par Φ. Puisque $\mathrm{P}(G)^{Q}$ et H sont commensurables et que $\mathrm{P}(D)$ est contenu dans $\mathrm{P}(G)^{Q}$, $H \cap \mathrm{P}(D)$ est d'indice fini dans $\mathrm{P}(D)$. Donc $\Phi(H) \cap \mathrm{P}_0(D)$ est d'indice fini dans $\mathrm{P}_0(D)$. Puisque $\mathrm{P}_0(D)$ est uniforme dans $\mathrm{P}_0(G)$ et que $\mathrm{P}(G) \cap H^{R}$ est d'indice fini dans H^{R}, $\Phi(H) \cap \mathrm{P}_0(D)$ est uniforme dans $\Phi(H)^{R}$. Puisque le noyau de P_0 contient $\tilde{N}, \Phi(H) = \Phi(S)$. Par le Lemme 7, la représentation Φ de S est équivalent à la représentation identique de S sur le corps des nombres rationnels. Donc le Lemme 8 entraîne que S^{Z} est uniforme dans S^{R}. On a donc vu la deuxième condition satisfaite.

6°) Soit f l'homomorphisme canonique de $\tilde{N}$ sur N. Le rang du noyau de f est égal à $\dim K$. Le noyau de f est donc contenu et uniforme dans le sous-groupe analytique de $\tilde{G}$ correspondant à $\mathfrak{k}$, et par suite $\tilde{D} \cap \tilde{K}$ est uniforme dans $\tilde{K}$. Il existe donc un système libre de générateurs $y_{t+1}, \cdots, y_n$ de $\tilde{D} \cap \tilde{K}$ tel que, si on pose $y_i = \exp Y_i$ $(t+1 \leqq i \leqq n)$, les éléments $Y_{t+1}, \cdots, Y_n$ forment une base de $\mathfrak{k}$. D'un autre côté, $(D \cap \tilde{N})K$ est fermé dans $\tilde{N}$ et il existe un système libre de générateurs $y_1^{*}, \cdots, y_t^{*}$ de $(\tilde{D} \cap \tilde{N})\tilde{K}/\tilde{K}$. Soit y_i $(1 \leqq i \leqq t)$ une image réciproque de y_i^{*} dans $\tilde{D} \cap \tilde{N}$, et soit Y_i $(1 \leqq i \leqq t)$ l'élément de $\mathfrak{n}$ tel que $y_i = \exp Y_i$. Alors les éléments $y_1, \cdots, y_n$ forment un système libre de générateurs de $\tilde{D} \cap \tilde{N}$ et les éléments $Y_1, \cdots, Y_n$ forment une base $\mathscr{B}$ de $\mathfrak{n}$ adaptée à la série normale $\mathfrak{n}$, $\mathfrak{k}$, $\{0\}$ de $\mathfrak{n}$. Puisque $x_1, \cdots, x_n$ est un système libre de générateurs de $\tilde{D} \cap \tilde{N}$, l'élément y_i $(1 \leqq i \leqq n)$ se représente sous la forme $\prod_{j=1}^{n} x_j^{a_{ij}}$, où les a_{ij} sont des entiers. En vertu du Lemme 1, on obtient la relation $Y_i = \sum_{j=1}^{n} b_j X_j$, où les b_j sont des nombres rationnels. Les deux bases $\mathscr{B}$ et $\mathscr{B}'$ sont donc liées par une transformation rationnelle. Nous considérons maintenant tout endomorphisme de $\mathfrak{n}$ comme une matrice par rapport à $\mathscr{B}$. En vertu du Lemme 8, $\mathrm{P}(G)^{Z}$ est uniforme dans $\mathrm{P}(G)$ aussi pour $\mathscr{B}$. On a donc vu toutes les conditions voulues satisfaites.

7°) On se propose maintenant de démontrer la réciproque. Soit $\mathfrak{z}$ le centre de $\mathfrak{n}$. Il est à remarquer que $\mathfrak{z}$ contient $\mathfrak{k}$ et que $\mathfrak{z}$ est le noyau de ρ. On peut supposer par le Lemme 8 que notre base rationnelle $\mathfrak{B} = X_1, \cdots, X_r, Z_1, \cdots, Z_s$ est adaptée à la série normale $\mathfrak{n}$, $\mathfrak{z}$, $\mathfrak{k}$, $\{0\}$ de $\mathfrak{n}$ et que les éléments $Z_1, \cdots, Z_s$ forment une base de $\mathfrak{z}$ telle que les éléments $\exp Z_i$ $(1 \leqq i \leqq s)$ engendrent un sous-groupe dicret du centre Z de N. Désignons par $\mathfrak{n}^Q$ l'algèbre de Lie sur $\boldsymbol{Q}$ formée des combinaisons linéaires des membres de $\mathfrak{B}$ à coefficients rationnels. Le centre $\mathfrak{z}^Q$ de $\mathfrak{n}^Q$ est alors l'ensemble des combinations linéaires de $Z_1, \cdots, Z_s$ à coefficients rationnels. Soient H la composante irréductible de l'élément neutre de l'adhérence algégrique de $\mathrm{P}(G)^Q$ dans $GL(n, \boldsymbol{Q})$ et $H = S \cdot H_u$ une décomposition de Chevalley de H. Puisque les matrices de S sont toutes semi-simples et qu'elles transforment Z^Q sur lui-même, il existe un sous-espace $\mathfrak{m}^Q$ de $\mathfrak{n}^Q$ tel que $\mathfrak{n}^Q$ se décompose en somme directe de $\mathfrak{m}^Q$ et de $\mathfrak{z}^Q$, et que $\mathfrak{m}^Q$ soit stable par S.

8°) $H_u{}^Z$ est uniforme dans H^R d'après la Proposition 18 de T. Ono [8] et notre Lemme 2. Puisque $H_u{}^R$ est un groupe de Lie nilpotent connexe et simplement connexe (voir Corollaire 2, p. 125 de [1]) et contenu dans $\mathrm{P}(G)$, il existe des matrices unipotentes rationnelles $Y_1{}^*, \cdots, Y_r{}^*$ telles qu'elles forment une base de $\rho(\mathfrak{n}^Q)$ et que les éléments $y_i{}^* = \exp Y_i{}^*$ $(1 \leqq i \leqq r)$ constituent un système libre de générateurs de $H_u{}^Z$. Soit Y_i $(1 \leqq i \leqq r)$ l'élément de $\mathfrak{m}^Q$ tel que $\rho(Y_i) = Y_i{}^*$. Alors les éléments $Y_1, \cdots, Y_r, Z_1, \cdots, Z_s$ forment aussi une base rationnelle $\mathfrak{B}'$ de $\mathfrak{n}$.

Soit $y_i = \exp Y_i$ dans G. On a la relation $y_i{}^* y_j{}^* y_i{}^{*-1} = \prod_{k=1}^{r} y_k{}^{*a_{ijk}}$ $(1 \leqq i, j \leqq r)$, d'où la relation: $y_i y_j y_i^{-1} = \prod_{k=1}^{r} y_k{}^{a_{ijk}} v_{ij}$, v_{ij} étant un élément de Z. Il suit du Lemme 1 et de la rationalité de la base $\mathfrak{B}'$ que v_{ij} est de la forme $\exp \sum_{k=1}^{s} b_{ijk} Z_k$, où les b_{ijk} sont des nombres rationnels. Soit p un dénominateur commun des b_{ijk}, et posons $Z'_k = (1/p) Z_k$ et $z'_k = \exp Z'_k$. Alors v_{ij} est de la forme

$$\prod_{k=1}^{s} z'_k{}^{c_{ijk}},$$

où c_{ijk} sont des entiers. Il en résulte que les éléments $y_1, \cdots, y_r, z'_1, \cdots, z'_s$ engendrent un sous-groupe dicret et uniforme dans N.

9°) D'après le Lemme 6, $\mathfrak{g}$ se décompose en produit semi-direct d'une sous-algèbre commutative $\mathfrak{a}$ et de $\mathfrak{n}$. Alors $G = AN$, où A est le sous-groupe analytique de G correspondant à $\mathfrak{a}$. Désignons par P_A la restriction de P à A. Le noyau de P_A est discret et $\mathrm{P}_A(A) = \mathrm{P}(G) \cap S^R$. Soit $u_1{}^*, \cdots, u_l{}^*$ un système de générateurs de $S^Z \cap \mathrm{P}(G)$ et soit u_i $(1 \leqq i \leqq l)$ une image réciproque de u_i^* par P_A. Soit encore $u_{l+1}, \cdots, u_m$ un système de générateurs du noyau de P_A. Il est alors facile à voir que les éléments $u_1, \cdots, u_m$ engendrent l'image réciproque D_A de $S^Z \cap \mathrm{P}(G)$ par P_A, qui est un sous-groupe discret et uniforme dans A.

10°) Soit M l'ensemble des éléments de N de la forme $\exp X$, où $X \in \mathfrak{m}$. D'après le Lemme 9, tout élément de N peut s'écrire dans une seue façon comme le produit d'un élément de M et d'un élément de Z. En vertu de l'invariance de $\mathfrak{m}$ sous les opérations de S, l'élément $u_i y_j u_i^{-1} = \exp \mathrm{P}u_i(Y_j)$ $(1 \leqq i \leqq m, 1 \leqq j \leqq r)$ appartient à M. D'un autre côté, on a la relation $u_i^* y_j^* u_i^{*-1} = \prod_{k=1}^{r} y_k^{*a_{ijk}}$, d'où la relation: $u_i y_j u_i^{-1} = \prod_{k=1}^{r} y_k^{a_{ijk}} \cdot v_{ij}$, $v_{ij} \in Z$.

Par le Lemme 1 et par la rationalité de la base $Y_1, \cdots, Y_r, Z'_1, \cdots, Z'_r$, $\prod_{k=1}^{r} y_k^{a_{ijk}}$ est de la forme $\exp(\sum_{k=1}^{r} b_{ijk} Y_k + \sum_{k=1}^{s} c_{ijk} Z'_k)$, où les b_{ijk} et les c_{ijk} sont des nombres rationnels.

Soit q un dénominateur commun des c_{ijk}, et posons $Z''_k = (1/q) Z'_k$, $z''_k = \exp Z''_k$. On a alors $\exp \sum_{k=1}^{s} c_{ijk} Z'_k = \prod_{k=1}^{s} z''^{d_{ijk}}_k$, où les d_{ijk} sont des entiers.

L'expression $\prod y^{a_{ijk}} = (\exp \sum b_{ijk} Y_k) \cdot (\prod z''^{d_{ijk}}_k)$ fournit une décomposition suivant $N = MZ$. En vertu de l'unicité, on obtient que $v_{ij} = \prod z''^{-d_{ijk}}_k$.

On a en plus:

$$u_i z''_j u_i^{-1} = \exp \mathrm{P}u_i(Z''_j) = \exp(1/pq) \mathrm{P}u_i(Z_j).$$

Puisque $\mathrm{P}u_i$ est une matrice entière par rapport à la base $\mathfrak{B}$, on a $\mathrm{P}u_i(Z_j) = \sum_{k=1}^{s} a_{ijk} Z_k$, où les a_{ijk} sont des entiers. On obtient donc $u_i z''_j u_i^{-1} = \prod_{k=1}^{s} z''^{a_{ijk}}_k$.

11°) Soit D_N le sous-groupe discret et uniforme dans N engendré par les éléments $y_1, \cdots, y_r$, $z''_1, \cdots, z''_s$. Posons enfin D le sous-groupe de G engendré par D_A et D_N. Alors les règles de commutations entre des générateurs de D décrites dans 8° et 10° montrent que $D = D_A D_N$ et que D est discret. De l'autre côté, le Lemme 2 implique que D est uniforme dans G, ce qui achève la démonstration du Théorème 3'.

COROLLAIRE 1. *La condition* 2) *du Théorème* 3' *peut se remplacer par les deux conditions suivantes.*

3) $(\mathrm{P}(G)^Q)^R$ *est uniforme dans l'adhérence algébrique de* $\mathrm{P}(G)$ *dans* $GL(n, \boldsymbol{R})$.

4) *Soit H la composante irréductible de l'élément neutre de l'adhérence algébrique de $\mathrm{P}(G)^{Q}$ dans $GL(n, \boldsymbol{Q})$. Alors H n'admet pas de caractère rationnel non-trivial.*

C'est une conséquence immédiate du Théorème 3′ et du Théorème 2.

COROLLAIRE 2. *Soit G^* l'adhérence algébrique de $\mathrm{P}(G)$ dans $GL(n, \boldsymbol{R})$ et soit $G^* = S^* \cdot G_u^*$ une décomposition de Chevalley de G^*. Alors la condition 2) du Théorème 3′ peut se remplacer par les deux conditions suivantes.*

5) *H_u est algébriquement dense dans G_u^*.*

6) $\operatorname{rang} \mathrm{X}(S^*) = \operatorname{rang} S^{*Z}$.

Supposons en effet qu'il existe dans G un sous-groupe discret et uniforme. Puisque G_u^* est un groupe de Lie nilpotent connexe et simplement connexe et que $(\mathrm{P}(G)^{Q})^{R}$ est uniforme dans G^*, H_u est algébriquement dense dans G_u^*. Puisque H^R est uniforme dans G^* et que $\mathrm{X}(S^*) = \mathrm{X}(G)^*$, le Lemme 2 et la Proposition 6 entraînent la condition 6).

Si réciproquement les deux conditions sont satisfaites, le Lemme 2, la Proposition 6 et la Proposition 18 de Ono [8] impliquent que H^Z est uniforme dans G^R, ce qui démontre le Corollaire 2.

4. Structures kählériennes.

LEMME 10. *Soit V un espace vectoriel de dimension finie sur le corps des nombres réels, et soit $\mathfrak{F}$ une famille linéaire commutative formée de transformations linéaires semi-simples de V. Si $\mathfrak{F}$ transforme V sur lui-même, il existe un élément X de $\mathfrak{F}$ tel qu'il transforme V sur lui-même*

Soit $V = V_1 + \cdots + V_s$ une décomposition de V en somme directe de sous-espaces simples. Alors $\dim V_i$ est 1 ou 2, et il existe des éléments X_i $(1 \leqq i \leqq s)$ de $\mathfrak{F}$ tels que $X_i(V_i) = V_i$. On peut alors trouver une combinaison linéaire $X = \sum_{i=1}^{s} \xi_i X_i$ telle que $X(V) = V$.

THÉORÈME 4. *Soit G un groupe de Lie résoluble connexe et simplement connexe. Pour qu'il existe dans G un sous-groupe commutatif discret et uniforme, il faut et il suffit que les trois conditions suivantes soient satisfaites:*

1°) *l'algèbre dérivée $\mathfrak{g}'$ de l'algèbre de Lie $\mathfrak{g}$ de G est commutative;*

2°) *il existe une sous-algèbre $\mathfrak{h}$ de $\mathfrak{g}$ telle que $\mathfrak{g}$ se décompose en produit semi-direct de $\mathfrak{h}$ et de $\mathfrak{g}'$;*

3°) *l'image de G par sa représentation sur l'espace* $\mathfrak{g}'$ *déduite de sa représentation adjointe est compacte.*

S'il en est ainsi, il suit de là que:

(i) *le plus grand idéal nilpotent* $\mathfrak{n}$ *de* $\mathfrak{g}$ *est commutatif, et* $\mathfrak{n}$ *se décompose en produit direct de* $\mathfrak{g}'$ *et du centre de* $\mathfrak{g}$.

(ii) *la série centrale décroissante de* $\mathfrak{g}$ *se termine avec* $\mathfrak{g}'$; *c'est-à-dire,* $[\mathfrak{g},\mathfrak{g}']=\mathfrak{g}'$. *Donc* $\mathfrak{g}'$ *est de dimension paire.*

Supposons d'abord les trois conditions satisfaites. Soit H le sous-groupe analytique de G correspondant à $\mathfrak{h}$, et soit Φ la représentation de H sur l'espace $\mathfrak{g}'$ déduite de la représentation adjointe de G. Alors le noyau de Φ est uniforme dans H d'après la condition 3°, et il existe une base $X_1,\cdots,X_s$ de $\mathfrak{h}$ telle que $\Phi\ (\exp X_i)=1$ pour $1\leqq i\leqq s$. Prenons du reste une base $X_{s+1},\cdots,X_n$ de $\mathfrak{g}'$. Alors les éléments $\exp X_i$ $(1\leqq i\leqq n)$ engendrent un sous-groupe commutatif discret et uniforme dans G.

Supposons ensuite que G contienne un sous-groupe commutatif discret et uniforme D. Désignons comme toujours par P of ρ respectivement les représentations de G et de $\mathfrak{g}$ sur $\mathfrak{n}$ qui se déduisent de leurs représentations adjointes. Soit N le sous-groupe analytique de G qui correspond à $\mathfrak{n}$. $D\cap N$ étant uniforme par le Théorème M, N est commutatif par la Proposition 4. Il existe une base $X_{r+1},\cdots,X_n$ de $\mathfrak{n}$ telle que les éléments $x_i=\exp X_i$ $(r<i\leqq n)$ forment un système libre de générateurs de $D\cap N$. Pour tout élément x de D, on a la relation $\exp Adx(X_i)=xx_ix^{-1}=x_i=\exp X_i$, et par suite $Adx(X_i)=X_i$. Donc $\mathrm{P}(D)=\{1\}$. De l'autre côté, $\mathrm{P}(N)=\{1\}$ puisque N est commutatif. $\mathrm{P}(G)$ s'identifie donc à l'image d'un espace compact G/DN par une application continue, ce qui implique que $\mathrm{P}(G)$ est compact. Soit G^∞ le dernier terme de la séries centrale décroissante de G. Alors le groupe DG^∞/G^∞ est un sous-groupe commutatif uniforme dans le groupe nilpotent simplement connexe G/G^∞. Donc G/G^∞ est commutatif, ce qui implique que $[\mathfrak{g},\mathfrak{g}']=\mathfrak{g}'$. Ce fait avec la semi-simplicité de la représentation ρ nous donne la décomposition de $\mathfrak{n}$ en produit direct de $\mathfrak{g}'$ et du centre de $\mathfrak{g}$.

Les éléments de $\rho(\mathfrak{g})$ restreints à $\mathfrak{g}'$ forment une famille linéaire de transformations linéaires semi-simples de $\mathfrak{g}'$, et en plus elle transforme $\mathfrak{g}'$ sur luimême. Il existe d'après le Lemme 10 un élément L de $\mathfrak{g}$ tel que $[L,\mathfrak{g}']=\mathfrak{g}'$. Soit $\mathfrak{h}$ le centralisateur de L dans $\mathfrak{g}$. Il est évident que $\mathfrak{h}\cap\mathfrak{g}'=\{0\}$. Si X est un élément de $\mathfrak{g}$, il existe un élément Y de $\mathfrak{g}'$ tel que $[L,X]=[L,Y]$. Donc $X-Y$ appartient à $\mathfrak{h}$, ce qui dit que $\mathfrak{g}$ est la somme directe des sous-espaces $\mathfrak{h}$ et de $\mathfrak{g}'$. Si X, Y sont des éléments de $\mathfrak{h}$, on a la relation $[L,[X,Y]] = [[L,X],Y] - [[L,Y],X] = 0$. Donc $\mathfrak{h}$ est une sous-algèbre de $\mathfrak{g}$. En plus, $\mathfrak{h}$ est commutative puisqu'elle est isomorphe à $\mathfrak{g}/\mathfrak{g}'$. Le Théorème 4 est donc démontré.

COROLLAIRE. *Les notations étant celles du Théorème 4, on peut prendre une base* L_i $(1 \leqq i \leqq r)$ *de* $\mathfrak{h}$ *et une base* A_j, B_j $(1 \leqq j \leqq t)$ *de* $\mathfrak{g}'$ *de telle sorte que l'on ait les relations de structure* $[L_i, A_j] = a_{ij}B_j$, $[L_i, B_j] = -a_{ij}A_j$, *où* a_{ij} *sont des entiers.*

Remarque. Soient G, N, Z et Z_0 respectivement un groupe de Lie résoluble connexe et simplement connexe, le plus grand sous-groupe analytique distingué nilpotent de G, le centre de G et sa composante connexe de l'élément neutre. On a alors l'inégalité suivante [9];

$$\operatorname{rang} Z/Z_0 \leqq \dim G - \dim N.$$

Il est donc évident que pour le group dans le Théorème 4, le rang en question est égal à $\dim G - \dim N$.

LEMME 11. *Soit G un groupe de Lie nilpotent connexe de matrices réelles. Si G contient un sous-groupe commutatif et uniforme, G est lui-même commutatif.*

Il est bien connu que G est le produit direct du plus grand sous-groupe compact K et d'un sous-groupe connexe et simplement connexe A. Soit D un sous-groupe commutatif et uniforme dans G. DK/K est un sous-groupe commutatif et uniforme dans G/K. La Proposition 4 implique donc que G/K est commutatif. A étant isomorphe à G/K, G est lui-même commutatif, ce qui finit la démonstration.

Le Théorème suivant est dû à J. Hano [2], qui n'y est d'ailleurs pas explicitement mentionné.

THÉORÈME H. *Soit G un groupe de Lie unimodulaire connexe et simplement connexe de dimension paire. Pour que G admette une structure kählerienne invariante à droite, il faut et il suffit que les conditions suivantes soient satisfaites:*

1°) *l'algèbre dérivée* $\mathfrak{g}'$ *de l'algèbre de Lie* $\mathfrak{g}$ *de* G *est commutative;*

2°) *il existe une sous-algèbre* $\mathfrak{h}$ *de* $\mathfrak{g}$ *telle que* $\mathfrak{g}$ *se décompose en produit semi-direct de* $\mathfrak{h}$ *et de* $\mathfrak{g}'$*;*

3°) *l'image de G par sa représentation sur $\mathfrak{g}'$ déduite de sa représentation adjointe a l'adhérence compacte dans $GL(\mathfrak{g}')$*;

4°) *la série centrale décroissante de $\mathfrak{g}$ se termine à $\mathfrak{g}'$.*

On obtient trivialement le corollaire suivant du Théorème 4 et du Théorème H.

COROLLAIRE. *Si un groupe de Lie résoluble connexe et simplement connexe de dimension paire contient un sous-groupe commutatif discret et uniforme, il admet une structure kählérienne invariante à droite. Si en particulier G est unimodulaire et si l'image de G par sa représentation sur l'espace $\mathfrak{g}'$ déduite de sa représentation adjointe est fermée dans $GL(\mathfrak{g}')$, la réciproque est aussi vraie.*

THÉORÈME 5. *Soit G un groupe algébrique résoluble d'automorphismes d'un espace vectoriel de dimension finie sur le corps des nombres réels. Alors les conditions (a) et (b) ci-dessous sont équivalentes. Si en particulier la dimension de G est paire, elles sont équivalentes à la condition (c).*

(a) *G contient un sous-groupe commutatif discret et uniforme*;

(b) *G satisfait aux trois conditions dans le Théorème 4*;

(c) *G est unimodulaire et admet une structure kählerienne invariante à droite.*

Remarquons d'abord que l'image de G par sa représentation sur $\mathfrak{g}'$ déduite de sa représentation adjointe est fermée dans $GL(\mathfrak{g}')$ par le Lemme 5. Désignons par G_0 la composante connexe de l'élément neutre de G et par $\tilde{G}$ le revêtement universel de G_0.

Supposons d'abord la condition (b) satisfaite. Alors $\tilde{G}$ satisfait aussi à (b). Soient H et $\tilde{H}$ les sous-groupes analytiques correspondant à $\mathfrak{h}$ dans G_0 et $\tilde{G}$ respectivement; et soient Z et Z_0 le centre de $\tilde{G}$ et sa composante connexe de l'élément neutre. Puisque rang Z/Z_0 ne peut pas dépasser $\dim \mathfrak{g} - \dim \mathfrak{n}$, Z doit être contenu dans $\tilde{H}$. Donc H est fermé dans G_0. Alors notre argument dans la démonstration du Théorème 4 reste valable sans aucune modification, et (b) entraîne (a).

Supposons ensuite la condition (a) satisfaite. On peut supposer que G_0 contient un sous-groupe commutatif discret et uniforme D. Soit N le sous-groupe analytique de G_0 correspondant à $\mathfrak{n}$. Le Théorème M dit que $D \cap N$ est uniforme dans N. N étant un groupe nilpotent connexe de matrices réelles, le Lemme 11 implique que N est commutatif. On voit alors facilement que $P(G)$ est compact, comme dans la démonstration du Théorème 4. Soit G^∞ le dernier terme de la série centrale décroissante de G. Puisque G est algébrique, G^∞ est aussi algébrique (voir [1]) et donc fermé dans G. Alors le groupe DG^∞/G^∞ est un sous-groupe commutatif et uniforme dans G/G^∞. Puisque G/G^∞ est isomorphe à un groupe algébrique nilpotent de matrices réelles (voir [1]), le Lemme 11 implique que G/G^∞ est commutatif, ce qui entraîne que $[\mathfrak{g}, \mathfrak{g}'] = \mathfrak{g}'$. Le reste de la démonstration est tout à fait le même que la dernière partie de celle du Théorème 4. Donc (a) entraîne (b).

Supposons enfin la dimension de G paire. La condition (c) équivaut à dire que $\tilde{G}$ est unimodulaire et admet une structure kählérienne invariante à droite. Alors le Théorème 4 et le Corollaire du Théorème H établissent l'équivalence de (c) et (b). Le Théorème 5 est donc démontré.

5. Une construction d'une variété abélienne. On se propose maintenant de construire une variété abélienne à partir d'une structure kählérienne invariante à droite sur un groupe de Lie résoluble connexe et simplement connexe. Soit G un tel groupe et $\mathfrak{g}$ son algèbre de Lie. Une structure kählérienne invariante sur G est donnée par une paire (J, B) d'une transformation linéaire J de $\mathfrak{g}$ appelée la structure complexe de $\mathfrak{g}$ et d'une forme bilinéaire symétrique positive non-dégénérée B sur $\mathfrak{g} \times \mathfrak{g}$ à valeurs réelles appelée la métrique kählérienne sur $\mathfrak{g}$, lesquelles satisfont ensemble aux conditions suivantes:

$$\begin{aligned}
&J^2 = -1,\\
&J[X,Y] - [JX,Y] - [X,JY] - J[JX,JY] = 0, \quad X, Y \in \mathfrak{g},\\
&B(JX,JY) = B(X,Y), \quad X, Y \in \mathfrak{g},\\
&dK = 0,
\end{aligned}$$

où $K(X,Y) = B(JX,Y)$ et K est considéré comme une cochaîne de degré 2 sur $\mathfrak{g}$.

Soit $\mathfrak{h}$ le sous-espace de $\mathfrak{g}$ complémentaire orthogonal à l'algèbre dérivée $\mathfrak{g}'$ par rapport à B. Alors $\mathfrak{h}$ est une sous-algèbre de $\mathfrak{g}$, et $\mathfrak{g}$ se décompose en produit semi-direct de $\mathfrak{h}$ et de $\mathfrak{g}'$ (voir [2]). Il existe donc une base L_i $(1 \leqq i \leqq r)$ de $\mathfrak{h}$ et une base A_j, B_j $(1 \leqq j \leqq t)$ de $\mathfrak{g}'$ telle qu'on ait les relations de structure

$$[L_i, A_j] = a_{ij} B_j, \qquad [L_i, B_j] = -a_{ij} A_j,$$

où a_{ij} sont des nombres réels, qui ne sont pas nécessairement rationnels. On désignera cette base par $\mathfrak{B}$.

D'après J. Hano [2], les sous-espaces $\mathfrak{h}$ et $\mathfrak{g}'$ sont respectivement stables par J. Donc les restrictions de (J, B) à $\mathfrak{h}$ et à $\mathfrak{g}'$ donnent respectivement des structures kählériennes sur H et sur G', où H et G' sont les sous-groupes analytiques de G correspondant à $\mathfrak{h}$ et à $\mathfrak{g}'$ respectivement. Nous montrerons d'abord que la variété kählerienne G se décompose en produit direct des deux variétés kählériennes H et G'.

Tout élément x de G s'écrit dans une seule façon sous la forme suivante:

$$x = \exp X \cdot \exp C, \qquad X = \sum_{i=1}^{r} x_i L_i, \qquad C = \sum_{j=1}^{t} (u_j A_j + v_j B_j).$$

Prenons deux bases de l'espace tangent à G en x. La première est la translatée à droite de la base $\mathfrak{B}$ de $\mathfrak{g}$. Les fonctions définies autour de x seront considérées comme fonctions de n variables réelles définies autour du point $(x_1, \cdots, x_r, u_1, v_1, \cdots, u_t, v_t)$. Leurs différentiations partielles par rapport à chaque variable forment la deuxième base. Remarquons ici que la deuxième base est adaptée à la décomposition de la variété G en produit direct des deux variétés H et G'. On obtient aisément la matrice de transition de ces deux bases:

$$\begin{array}{c} r\left\{\begin{array}{c} \\ \\ \\ \end{array}\right. \\ 2t\left\{\begin{array}{c} \\ \\ \\ \\ \end{array}\right. \end{array}
\left(\begin{array}{ccc|ccc}
1 & & & & & \\
 & \ddots & & & & \\
 & & 1 & & & \\ \hline
 & & & \begin{array}{|cc|}\hline \cos a_1 & -\sin a_1 \\ \sin a_1 & \cos a_1 \\ \hline \end{array} & & \\
 & & & & & \cdots \\
 & & & & & \cdots
\end{array}\right), \quad a_j = \sum_{i=1}^{r} x_i a_{ij}.$$

On obtient donc la décomposition de la variété kählérienne G en produit direct des deux variétés kählériennes H et G'

Nous posons désormais les deux hypothèses suivantes:

HYPOTHÈSE I. *L'image de G par sa représentation sur $\mathfrak{g}'$ déduite de sa représentation adjointe est fermée dans $GL(\mathfrak{g}')$.*

Alors le groupe G est du type traité dans le Théorème 4, et donc on suppose que les constantes de structure a_{ij} de la base $\mathfrak{B}$ soient toutes entières (voir Corollaire du Théorème 4).

HYPOTHÈSE II. *La matrice associée à la forme bilinéaire K par rapport à la base $\mathfrak{B}$ est rationnelle.*

Les éléments $\exp 2\pi L_i$ $(1 \leqq i \leqq r)$, $\exp A_j$, $\exp B_j$ $(1 \leqq j \leqq t)$ engendrent un sous-groupe commutatif discret et uniforme dans G. Nous le désignons par D. Sous ces hypothèses, nous allons montrer que la variété G/D sera munie d'une structure de variété abélienne déduite de la structure kählérienne sur G.

D est le produit direct de $D \cap H$ et de $D \cap G'$. Puisque $D \cap H$ est central dans G, la variété quotient G/D se décompose en produit direct des deux variétés $H/D \cap H$ et $G'/D \cap G'$. Donc la variété kählérienne quotient G/D est le produit direct des deux tores kählériens $H/D \cap H$ et $G'/D \cap G'$.

On considère H comme espace vectoriel et définit une structure complexe J de H par $J_x = \exp 2\pi JX$, où $x = \exp 2\pi X$, $X \in \mathfrak{h}$. On définit une forme bilinéaire E sur $H \times H$ *par* $E(x, y) = -K(X, Y)$, où $x = \exp 2\pi X$, $y = \exp 2\pi Y$, $X, Y \in \mathfrak{h}$. Il est alors facile de vérifier les conditions de Riemann pour E, de sorte que $H/D \cap H$ est une variété abélienne. Il en est de même de $G'/D \cap G'$. La variété G/D est donc le produit direct de deux variétés abéliennes.

Exemple. Supposons que l'hypothèse I se vérifie pour G. Prenons la matrice unité pour matrice associée à la forme bilinéaire B et la matrice

$$\begin{pmatrix} \begin{array}{cc|} 0 & -1 \\ 1 & 0 \\ \hline \end{array} & & \\ & \boxed{\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array}} & \\ & & \begin{matrix} \cdot\cdot\cdot\cdot \\ \cdot\cdot\cdot\cdot \\ \cdot\cdot\cdot\cdot \end{matrix} \end{pmatrix}$$

pour matrice de la transformation linéeaire J, toutes les deux par rapport à la base $\mathfrak{B}$. On voit facilement que (J, B) donne une structure kählerienne invariante à droite sur G et que l'hypothèse II se vérifie.

UNIVERSITÉ DE TOKYO, UNIVERSITÉ DE PARIS.

BIBLIOGRAPHIE.

[1] C. Chevalley, *Théorie des groupes de Lie III*, Actualités Scientifiques et Industrielles, No. 1226, Paris, 1955.

[2] J. Hano, "On kaelerian homogeneous spaces of unimodular Lie groups," *American Journal of Mathematics*, vol. 76 (1957), pp. 885-900.

[3] A. I. Malcev, "On a class of homogeneous spaces," *Isvestiya Akademii Nauk SSSR, Seriya Matematičeskaya*, vol. 13 (1949), pp. 9-32 (en russe); *American Mathematical Society Translation* No. 39 (1951).

[4] Y. Matsushima, "On the discrete subgroups and homogeneous spaces of nilpotent Lie groups," *Nagoya Mathematical Journal*, vol. 2 (1951), pp. 95-110.

[5] G. D. Mostow, "Factor spaces of solvable groups," *Annals of Mathematics*, vol. 60 (1954), pp. 1-27.

[6] ———, "Self adjoint groups," *ibid.*, vol. 62 (1955), pp. 44-55.

[7] ———, "On the fundamental group of a homogeneous space," *ibid.*, vol. 66 (1957), pp. 249-255.

[8] T. Ono, "On some arithmetic properties of linear algebraic groups," *ibid.*, vol. 70 (1959), pp. 266-290.

[9] M. Saito, "Sur certains groupes de Lie résolubles I et II," *Scientific Papers of the College of General Education. University of Tokyo*, vol. 7 (1957), pp. 1-11, pp. 157-168.

[10] ———, "Sur certains groupes résolubles," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, vol. 248 (1959), pp. 1909-1911.

[11] *Séminaire "Sophus Lie"* 1954/55, Exposé No. 22, 1955.

[12] A. Weil, *Discontinuous subgroups of classical groups*, Lecture notes, University of Chicago, 1958.

A COMBINATORIAL GENERALIZATION OF THE ROGERS-RAMANUJAN IDENTITIES.*

By Basil Gordon.

---

1. Introduction. The Rogers-Ramanujan identities (cf. [1], p. 290) state that

$$(1) \quad \sum_{n=0}^{\infty} 1/(1-x^{5n+1})(1-x^{5n+4}) = \sum_{m=0}^{\infty} x^{m^2}/(1-x)(1-x^2)\cdots(1-x^m)$$

and

$$(2) \quad \sum_{n=0}^{\infty} 1/(1-x^{5n+2})(1-x^{5n+3}) = \sum_{m=0}^{\infty} x^{m^2+m}/(1-x)(1-x^2)\cdots(1-x^m).$$

Identity (1) can be interpreted combinatorially as saying that the number of partitions of any integer N into parts not congruent to 0, $\pm 2 \pmod 5$ is equal to the number of partitions of $N = N_1 + N_2 + \cdots + N_k$ with $N_i \geqq N_{i+1} + 2$. Similarly, identity (2) says that the number of partitions of N into parts not congruent to 0, $\pm 1 \pmod 5$ is equal to the number of partitions $N = N_1 + N_2 + \cdots + N_k$ with $N_i \geqq N_{i+1} + 2$, $N_k \geqq 2$. In view of Euler's identity

$$(3) \quad \begin{aligned} \prod_{n=0}^{\infty} 1/(1-x^{2n+1}) &= \prod_{n=1}^{\infty} (1+x^n) \\ &= \sum_{m=0}^{\infty} x^{(m^2+m)/2}/(1-x)(1-x^2)\cdots(1-x^m) \end{aligned}$$

which says that the number of partitions of N into odd parts is equal to the number of partitions of N into unequal parts, one is naturally led to look for generalizations of (1), (2), and (3). It is tempting to suppose that such an extension would involve partitions of the form $N = N_1 + \cdots + N_k$ with $N_i \geqq N_{i+1} + d$ $(d \geqq 3)$, and Schur [8] has obtained such a result for $d = 3$. However, Lehmer [2] and Alder [3] have proved several non-existence theorems about this type of generalization. On the other hand Glaisher [4] proved the following extension of Euler's identity (3).

Glaisher's Theorem. The number of partitions of any integer N into parts not divisible by d is equal to the number of partitions of the form $N = N_1 + \cdots + N_k$ with $N_i \geqq N_{i+1}$ and $N_i \geqq N_{i+d-1} + 1$.

We will obtain the corresponding extension of (1) and (2) by proving

---

* Received January 3, 1961.

THEOREM 1. *The number of partitions of N into parts not congruent to* $0, \pm t \pmod{2d+1}$, *where* $1 \leqq t \leqq d$, *is equal to the number of partitions of the form* $N = N_1 + \cdots + N_k$, *where* $N_1 \geqq N_{i+1}$, $N_i \geqq N_{i+d-1} + 2$, *and* $N_{k-t+1} \geqq 2$.

Alder [6] and Singh [9] have obtained an *analytical* generalization of the Rogers-Ramanujan identities to the effect that

$$(4) \qquad \prod_{\substack{n=1 \\ n \not\equiv 0, \pm t (2d+1)}}^{\infty} 1/(1-x^n) = 1 + \sum_{m=1}^{\infty} P_{d,t,m}(x)/(1-x)\cdots(1-x^m),$$

where the $P_{d,t,m}(a)$ are polynomials in x. Carlitz [7] has recently obtained an explicit formula for these polynomials when $t = 1$ or $t = d$. I have not been able to show directly that the right hand side of (4) is the generating function for partitions $N = N_1 + \cdots + N_k$, where $N_i \geqq N_{i+1}$, $N_i \geqq N_{i+d-1} + 2$, and $N_{k-t+1} \geqq 2$ even in the special cases $t = 1$ and $t = d$. Theorem 1 suggests strongly that such an interpretation is possible.

2. Proof of Theorem 1. The method of proof is similar to that of Schur [5] for (1) and (2). Denote by $F_{dt}(N)$ the number of partitions of the form $N = N_1 + \cdots + N_k$, where $N_i \geqq N_{i+1}$, $N_i \geqq N_{i+d-1} + 2$, and $N_{k-t+1} \geqq 2$. Put $F_{dt}(0) = 1$, and consider the generating function $\phi_{dt}(x) = \sum_{n=0}^{\infty} F_{dt}(N) x^N$. For example $\phi_{21}(x)$ and $\phi_{22}(x)$ are the right hand sides of (2) and (1) respectively. To prove Theorem 1 we must show that

$$(5) \qquad \phi_{dt}(x) = \prod_{n=1}^{\infty} (1 - x^{(2d+1)n})(1 - x^{(2d+1)n-t})(1 - x^{(2d+1)n-2d-1+t})/(1-x^n),$$

since the right hand side of (4) is the generating function for the number of partitions of N into parts not congruent to $0, \pm t \pmod{2d+1}$. In Jacobi's identity

$$\prod_{\mu=1}^{\infty} (1 - q^{2\mu})(1 + q^{2\mu-1}z)(1 + q^{2\mu-1}z^{-1}) = \sum_{-\infty}^{\infty} q^{\nu^2} z^{\nu},$$

take $q = x^{d+\frac{1}{2}}$ and $z = -x^{d-t+\frac{1}{2}}$. This gives the identity

$$\prod_{\mu=1}^{\infty} (1 - x^{(2d+1)\mu})(1 - x^{(2d+1)\mu-t})(1 - x^{(2d+1)\mu-2d-1+t}) = \sum_{\nu=-\infty}^{\infty} (-1)^{\nu} x^{\alpha(\nu)},$$

where $\alpha(\nu) = (d+\frac{1}{2})\nu^2 + (d-t+\frac{1}{2})\nu$.

It is therefore sufficient to prove that

$$\prod_{\mu=1}^{\infty}(1-x^{\mu})\phi_{dt}(x)=\sum_{-\infty}^{\infty}(-1)^{\nu}x^{\alpha(\nu)}.$$

When the left hand side of (6) is expanded as a power series $\sum_{n=0}^{\infty} c_{dt}(n)x^n$, the coefficients $c_{dt}(n)$ can evidently be interpreted as follows: write $n=a_1+\cdots+a_k+b_1+\cdots+b_l$, where

$$(7) \qquad a_i \geqq a_{i+1}+1, \quad b_j \geqq b_{j+1}, \quad b_j \geqq b_{j+d-1}+2, \quad b_{l-t+1} \geqq 2.$$

Then $c_{dt}(n)=\sum(-1)^k$, the sum being extended over all such partitions. We will show wthat there is a 1: 1 correspondence between the class of all such partitions with k even and the class of those with k odd except when n has the form

$$n=(d+\tfrac{1}{2})\nu^2+(d-t+\tfrac{1}{2})\nu \qquad (\nu=0,\pm 1,\pm 2,\cdots).$$

In this case we will prove that the class for which $k\equiv\nu(2)$ contains one more partition than the class for which $k\not\equiv\nu(2)$. This of course proves that $c_{dt}(n)=0$ unless $n=(d+\frac{1}{2})\nu^2+(d-t+\frac{1}{2})\nu$, in which case $c_{dt}(n)=(-1)^{\nu}$; the theorem then follows at once.

As in [5], we write any partition satisfying conditions (7) in the form $(A \mid B)=(a_1\cdots a_k \mid b_1\cdots b_l)$; if the a's or b's are absent from the partition, it is denoted by $(-\mid B)$ or $(A\mid -)$. For example if $d=3$, $t=1$, $n=6$, the partitions in question are $(6\mid -)$, $(51\mid -)$, $(42\mid -)$, $(321\mid -)$, $(4\mid 2)$, $(31\mid 2)$, $(3\mid 3)$, $(21\mid 3)$, $(2\mid 4)$, $(2\mid 22)$, $(1\mid 5)$, $(1\mid 32)$, $(-\mid 6)$, $(-\mid 42)$, $(-\mid 33)$. It s convenient to call partitions satisfying (7) *admissible,* and to speak of them as even or odd according as k is even or odd. If both $(a_1\cdots a_k \mid b_1\cdots b_l)$ and $(a_2\cdots a_k \mid a_1b_1\cdots b_l)$ are admissible, they are paired with each other as the first step in setting up the correspondence between even and odd partitions. Thus in the above example we would have the pairs $(6\mid -)\leftrightarrow(-\mid 6)$, $(51\mid -)\leftrightarrow(1\mid 5)$, $(42\mid -)\leftrightarrow(2\mid 4)$, $(321\mid -)\leftrightarrow(21\mid 3)$, $(4\mid 2)\leftrightarrow(-\mid 42)$, $(31\mid 2)\leftrightarrow(1\mid 32)$, $(3\mid 3)\leftrightarrow(-\mid 33)$, leaving only $(2\mid 22)$ without a mate.

After this preliminary matching, we are left with the set $\mathfrak{A}$ of admissible partitions $(a_1\cdots a_k \mid b_1\cdots b_l)$ such that neither $(b_1a_1\cdots a_k \mid b_2\cdots b_l)$ nor $(a_2\cdots a_k \mid a_1b_1\cdots b_l)$ is admissible. Such a partition must clearly satisfy $b_1\leqq a_1\leqq b_{d-1}+1$. We first subdivide $\mathfrak{A}$ into the disjoint subsets $\mathfrak{A}_i$ $(1\leqq i\leqq d)$, where the partitions of $\mathfrak{A}_i$ satisfy

$$a_1=b_1=\cdots=b_{i-1}=b_i+1=\cdots=b_{d-1}+1.$$

Here the usual conventions are made when $i = 1$ or d, i. e. in $\mathfrak{A}_1$ we have $a_1 = b_1 + 1 = \cdots = b_{d-1} + 1$, and in $\mathfrak{A}_d$, $a_1 = b_1 = \cdots = b_{d-1}$. We next define three characteristic numbers p, q, r for the partition $(a_1, \cdots, a_k \mid b_1 \cdots b_l)$ as follows: $p = a_k$, q is the largest integer such that $a_1 - a_2 = a_2 - a_3 = \cdots = a_{q-1} - a_q = 1$, and r is the largest integer such that $b_{d-1} - b_{2(d-1)} = \cdots = b_{(r-1)(d-1)} - b_{r(d-1)} = 2$. In the case of the sets $\mathfrak{A}_2, \cdots, \mathfrak{A}_{d-1}$ there is a fourth characteristic number s, defined to be the largest integer such that $b_{i-1} - b_{i-1+(d-1)} = \cdots = b_{i-1+(s-2)(d-1)} - b_{i-1+(s-1)(d-1)} = 2$. For example if $d = 3$, then the partition $(4 \mid 4422)$ is in $\mathfrak{A}_3$, and has characteristic numbers $(4, 1, 2)$, while $(43 \mid 431)$ is in $\mathfrak{A}_2$ and has characteristic numbers $(3, 2, 1, 1)$. Now let ν be the minimum of the characteristic numbers of any given partition. We divide $\mathfrak{A}_1$, $\mathfrak{A}_d$ into 3 classes, and $\mathfrak{A}_2, \cdots, \mathfrak{A}_{d-1}$ into 4 classes according to which characteristic number attains this minimum as follows (here $2 \leqq i \leqq d-1$):

$$\begin{array}{rl}
\mathfrak{A}_1{}': & p = \nu, q \geqq \nu, r \geqq \nu, \\
\mathfrak{A}_1{}'': & p > \nu, q = \nu, r \geqq \nu, \\
\mathfrak{A}_1{}''': & p > \nu, q > \nu, r = \nu, \\
\mathfrak{A}_d{}': & p = \nu, q \geqq \nu, r \geqq \nu, \\
\mathfrak{A}_d{}'': & p > \nu, q \geqq \nu, r = \nu, \\
\mathfrak{A}_d{}^{\mathrm{iv}}: & p > \nu, q = \nu, r > \nu, \\
\mathfrak{A}_i{}': & p = \nu, q \geqq \nu, r \geqq \nu, \\
\mathfrak{A}_i{}'': & p > \nu, q \geqq \nu, r \geqq \nu, s = \nu, \\
\mathfrak{A}_i{}''': & p > \nu, q = \nu, r \geqq \nu, s > \nu, \\
\mathfrak{A}_i{}^{\mathrm{iv}}: & p > \nu, q > \nu, r = \nu, s > \nu.
\end{array}$$

Thus in the above examples, $(4 \mid 4422) \in \mathfrak{A}_3{}^{\mathrm{iv}}$, and $(43 \mid 431) \in \mathfrak{A}_2{}''$. We now define 3 mappings U, V, W and their inverses as follows. If

$$\pi = (a_1, \cdots, a_k \mid b_1, \cdots, b_l) \in \mathfrak{A}_1{}'',$$

put $U(\pi) = (a_1 - 1, a_2 - 1, \cdots, a_\nu - 1, a_{\nu+1}, \cdots, a_k, \nu \mid b_1, \cdots, b_l)$. This always leads to a partition of $\mathfrak{A}_d{}'$ unless $k = \nu$ and $a_\nu - 1 = \nu$. Then since $q = \nu$ and $r \geqq \nu$, π has the form

$$(2\nu, 2\nu - 1, \cdots, \nu + 1 \mid \overbrace{2\nu - 1, 2\nu - 1, \cdots, 2\nu - 1}^{d-1},$$
$$\overbrace{2\nu - 3, \cdots, 2\nu - 3}^{d-1}, \cdots, \overbrace{1, \cdots, 1}^{d-1}),$$

and so $n = 2\nu(2\nu + 1)/2 - \nu(\nu + 1)/2 + (d - 1)\nu^2 = (d + \tfrac{1}{2})\nu^2 + \nu/2$. Conversely if $\pi \in \mathfrak{A}_d{}'$, then we can form

$$U^{-1}(\pi) = (a_1 + 1, \cdots, a_\nu + 1, a_{\nu+1}, \cdots, a_{k-1} \mid b_1, \cdots, b_l)$$

and we get an element of $\mathfrak{A}_1''$ unless $k = \nu$. Then, since $p = \nu$, $q \geqq \nu$, $r \geqq \nu$, we have

$$\pi = (2\nu - 1, 2\nu - 2, \cdots, \nu \,|\, \overbrace{2\nu - 1, \cdots, 2\nu - 1}^{d-1},$$
$$\overbrace{2\nu - 3, \cdots, 2\nu - 3}^{d-1}, \cdots, \overbrace{1, \cdots, 1}^{d-1}).$$

Thus

$$\begin{aligned} n &= (2\nu - 1)(2\nu)/2 - \nu(\nu + 1)/2 + (d - 1)\nu^2 \\ &= (d + \tfrac{1}{2})\nu^2 - \nu/2. \end{aligned}$$

If $\pi \in \mathfrak{A}_i'$ $(1 \leqq i \leqq d - 1)$ we put

$$V(\pi) = (a_1, \cdots, a_{k-1} \,|\, b_1, \cdots, b_{i-1}, b_i + 1, b_{i+1}, \cdots,$$
$$b_{i-1+(d-1)}, b_{i+(d-1)} + 1, \cdots, b_{i+(\nu-1)+(d-1)} + 1, \cdots).$$

Then $V(\pi) \in \mathfrak{A}_{i+1}''$. Conversely if $\pi \in \mathfrak{A}_{i+1}''$, then

$$V^{-1}(\pi) = (a_1, \cdots, a_k, \nu \,|\, b_1, \cdots, b_{i-1}, b_i - 1, \cdots, b_{i+(\nu-1)(d-1)} - 1, \cdots)$$

is in $\mathfrak{A}_i'$. However $V^{-1}(\pi)$ may fail to satisfy $b_{i-t+1} \geqq 2$. This happens if and only if $i = d - t$, $n = (d + \frac{1}{2})\nu^2 + (d - t + \frac{1}{2})\nu$ and

$$\pi = (2\nu, 2\nu - 1, \cdots,$$
$$\nu + 1 \,|\, \overbrace{2\nu, \cdots, 2\nu}^{d-1}, \overbrace{2\nu - 1, \cdots, 2\nu - 1}^{t-1}, \overbrace{2\nu - 2, \cdots, 2\nu - 2}^{d-1}, \cdots).$$

If $\pi \in \mathfrak{A}_i^{\text{iv}}$ $(2 \leqq i \leqq d)$, we define

$$W(\pi) = (b_1, a_1 - 1, \cdots, a_\nu - 1, a_{\nu+1}, \cdots, a_k \,|\, b_2, \cdots, b_{d-1}, b_d + 1,$$
$$b_{d+1}, \cdots, b_{2d-1} + 1 \cdots, b_{d+(\nu-1)(d-1)} + 1, \cdots).$$

Then $W(\pi) \in \mathfrak{A}_{i-1}'''$. Conversely if $\pi \in \mathfrak{A}_{i-1}'''$, then

$$W^{-1}(\pi) = (a_2 + 1, \cdots, a_{\nu+1} + 1, \cdots, a_k \,|\, a_1, b_1, \cdots,$$
$$b_{d-1} - 1, \cdots, b_{(\nu-1)(d-1)} - 1, \cdots) \in \mathfrak{A}_i^{\text{iv}}.$$

This time $W^{-1}(\pi)$ will violate the condition $b_{i-t+1} \geqq 2$ if and only if $t = i$,

$$n = (d + \tfrac{1}{2})\nu^2 - (d - t + \tfrac{1}{2})\nu,$$

and

$$\pi = (2\nu - 1, 2\nu - 2, \cdots, \nu \,|\, \overbrace{2\nu - 1, \cdots, 2\nu - 1}^{t-1}, \overbrace{2\nu - 2, \cdots, 2\nu - 2}^{d-t},$$
$$\overbrace{2\nu - 3, \cdots, 2\nu - 3}^{t-1}, \cdots).$$

Thus the correspondence is 1 : 1 except when $n = (d+\frac{1}{2})\nu^2 + (d-t+\frac{1}{2})\nu$ (ν positive or negative), and for the surplus partition $(a_1,\cdots,a_k \mid b_1,\cdots,b_l)$, k always has the same parity as ν. This completes the proof of the theorem. As the proof is necessarily rendered obscure by the notation, we give an example of the above correspondence when $d = 3$, $t = d$, $n = 17$. There are 38 partitions altogether, and they are grouped in classes below, with the image of each partition written opposite to it.

$\mathfrak{A}_1'$	(61 | 55)	$\xrightarrow{V}$	$\mathfrak{A}_2''$	(6 | 65)
	(531 | 44)			(53 | 54)
	(521 | 441)			(52 | 541)
	(51 | 4421)			(5 | 5421)
	(4321 | 331)			(432 | 431)
	(432 | 3331)			(43 | 4321)
$\mathfrak{A}_1''$	(6 | 551)	$\xrightarrow{U}$	$\mathfrak{A}_3'$	(51 | 551)
	(53 | 441)			(431 | 441)
	(52 | 442)			(421 | 442)
	(52 | 4411)			(421 | 4411)
	(5 | 4422)			(41 | 4422)
$\mathfrak{A}_1'''$	(54 | 44)	$\xleftarrow{W}$	$\mathfrak{A}_2^{\text{iv}}$	(5 | 543)
$\mathfrak{A}_2'$	(521 | 54)	$\xrightarrow{V}$	$\mathfrak{A}_3''$	(52 | 55)
	(51 | 542)			(5 | 552)
	(51 | 5411)			(5 | 5511)
	(4321 | 43)			(432 | 44)
	(431 | 432)			(43 | 442)
	(431 | 4311)			(43 | 4411)
	(421 | 4321)			(42 | 4421)
$\mathfrak{A}_2'''$	None		$\mathfrak{A}_3^{\text{iv}}$	None

In conclusion it may be noted that a similar extension of Schur's theorem on partitions ([8], Theorem V, p. 495) can be given. This will be shown elsewhere.

UNIVERSITY OF CALIFORNIA AT LOS ANGELES.

REFERENCES.

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 1960.

[2] D. H. Lehmer, "Two non-existence theorems on partitions," *Bulletin of the American Mathematical Society*, vol. 52 (1946), pp. 538-44.

[3] H. L. Alder, "The non-existence of certain identities in the theory of partitions and compositions," *ibid.*, vol. 54 (1948), pp. 712-722.

[4] J. W. L. Glaisher, "A theorem in partitions," *Messenger of Mathematics*, vol. 12 (1883), pp. 158-170.

[5] I. Schur, "Ein Beitrag zur additiven Zahlentheorie," *Akademie der Wissenschaften, Berlin, Sitzungsberichte*, 1917, pp. 302-(21.

[6] H. L. Alder, "Generalizations of the Rogers-Ramanujan identities," *Pacific Journal of Mathematics*, vol. 4 (1954), pp. 161-168.

[7] L. Carlitz, "Note on Alder's polynomials," *ibid.*, vol. 10 (1960), pp. 517-519.

[8] I. Schur, "Zur Additiven Zahlentheorie," *Akademie der Wissenschaften, Berlin, Sitzungsberichte*, 1926, pp. 488-495.

[9] V. N. Singh, "Certain generalized hypergeometric identities of the Rogers-Ramanujan type," *Pracific Journal of Mathematics*, vol. 7 (1957), pp. 1011-1014.

A FAMILY OF SIMPLE GROUPS ASSOCIATED WITH THE SIMPLE LIE ALGEBRA OF TYPE (F_4).*

By RIMHAK REE.[1]

Introduction. In [4] the author constructed a family of new simple groups by applying to the Chevalley groups of type (G_2) a method which was obtained by analyzing Suzuki groups [5]. In this paper, we obtain another family of simple groups, which also seem to be new,[2] by applying the same method to the Chevalley groups (F_4). The orders of the finite groups in the family are given by

$$q^{12}(q-1)(q^3+1)(q^4-1)(q^6+1),$$

where $q = 2^{2n+1}$, $n = 1, 2, 3, \cdots$.

The construction is based on a certain automorphism[3] of the Chevalley group of type (F_4) over a field of characteristic 2. The existence of such an automorphism is already suggested in [3, Exposé 24, pp. 4-5]. Our group turns out to be the group of invariant elements under the automorphism.

Throughout this paper, we shall use the notation of [4, Section 1].

1. The root system of type (F_4). The root system Σ of type (F_4) consists of the 48 roots:

$$(1.1) \qquad \xi_i, \quad \xi_i + \xi_j, \quad \tfrac{1}{2}(\xi_i + \xi_j + \xi_k + \xi_l),$$

where: $i, j, k, l = \pm 1, \pm 2, \pm 3, \pm 4$; $|i|$, $|j|$, $|k|$, $|l|$ are distinct; $\xi_{-i} = -\xi_i$ for all i.

Let P be the additive group generated by Σ, and $V = \mathbf{R} \otimes P$ the vector

---

* Received September 13, 1960; revised February 21, 1961.

[1] This work was done while the author held a Research Associateship, 1959-1960, of the Office of the Naval Research, U. S. Navy. The content of this paper, together with that of [4], was announced in a lecture given at the American Mathematical Society Summer Institute on Finite Groups, Pasadena, California, on August 22, 1960.

The author would like to express gratitude to J. Tits for his perusal of the manuscript and many valuable suggestions.

[2] J. Tits informs the author that he has proved, by treating the orders of the finite groups by Artin's method [6], that the finite groups in our family are actually new.

[3] The author learned at Pasadena that the idea of obtaining simple groups by using this automorphism was also conceived, independently, by Robert Steinberg.

space over the real number field $\boldsymbol{R}$. Define the positive definite metric $(\xi \mid \eta)$ of V by $(\xi_i \mid \xi_i) = 1$, $(\xi_i \mid \xi_j) = 0$ for $i, j = 1, 2, 3, 4$; $i \neq j$. Then one can verify that the number $s(r)$ defined in [4, Section 1] can be written $s(r) = 2(s \mid r)/(r \mid r)$. Hence for the element w_r in the Weyl group W of Σ, we have $w_r(s) = s - (2(s \mid r)/(r \mid r))r$ for all $s \in \Sigma$. From this it follows that W leaves the metric $(\xi \mid \eta)$ invariant. By (1.1) one can see easily that $(r \mid r) = 1$ or 2, and that $(r \mid s) = 0$ or ± 1 for any $r, s \in \Sigma$. We shall write $\lambda(r) = (r \mid r)$.

We shall prove a few lemmas which will be used later.

(1.2) If $r, s, r+s \in \Sigma$, $\lambda(r) = \lambda(s) = 2$, then $\lambda(r+s) = 2$.

Proof.

$$\lambda(r+s) = (r+s \mid r+s) = (r \mid r) + 2(r \mid s) + (s \mid s) = 4 + 2(r \mid s) = 1 \text{ or } 2.$$

Then, since $(r \mid s) = 0$ or ± 1, we must have $(r \mid s) = -1$, $\lambda(r+s) = 2$.

(1.3) If $r, s, r+s \in \Sigma$, $\lambda(r) = 1$, $\lambda(s) = 2$, then $2r+s \in \Sigma$, and $\lambda(r+s) = 1$, $\lambda(2r+s) = 2$.

Proof. $\lambda(r+s) = (r+s \mid r+s) = 3 + 2(r \mid s) = 1$ or 2. Since $(r \mid s) = 0$ or ± 1, we must have $(r \mid s) = -1$, $\lambda(r+s) = 1$. Then $\lambda(r-s) = 3 - 2(r \mid s) = 5$. Hence $r - s \notin \Sigma$. Then $s(r) = 2(s \mid r)/(r \mid r) = -2$ implies that $2r+s \in \Sigma$. We have $\lambda(2r+s) = 4 + 2 + 2(r \mid s) = 2$.

Now, define the linear map $\psi \colon V \rightarrow V$ by

$$\psi(\xi_1) = \xi_1 + \xi_2, \quad \psi(\xi_2) = \xi_1 - \xi_2, \quad \psi(\xi_3) = \xi_3 + \xi_4, \quad \psi(\xi_4) = \xi_3 - \xi_4.$$

Then we have (cf. [3], Exposé 24, pp. 4-5)

(1.4) There exists a permutation $r \rightarrow \bar{r}$ of order 2 of Σ such that $\psi(r) = \lambda(r)\bar{r}$, $\overline{-r} = -\bar{r}$, $\lambda(r)\lambda(\bar{r}) = 2$ for all $r \in \Sigma$.

By the definition of ψ, one can see easily that $\psi = \sqrt{2}\psi_\delta$, where ψ_δ is an orthogonal transformation (in fact, a symmetry) of the vector space V. From this and (1.4) we have

(1.5) $\lambda(s)(\bar{r} \mid \bar{s}) = \lambda(\bar{r})(r \mid s)$ for all $r, s \in \Sigma$.

(1.6) $\overline{w_r(s)} = w_{\bar{r}}(\bar{s})$ for all $r, s \in \Sigma$.

Proof. This follows easily from (1.5).

(1.7) The map $w \rightarrow \bar{w} = \psi \circ w \circ \psi^{-1}$ is an automorphism of the Weyl group W such that $\overline{w_r} = w$ for all $r \in \Sigma$.

Proof. This is immediate from (1.6).

(1.8) If $r, s, r+s \in \Sigma$, and $\bar{r}+\bar{s} \notin \Sigma$, then $\lambda(r)=\lambda(s)=1, \lambda(r+s)=2$.

Proof. Since $\bar{r}+\bar{s} \notin \Sigma$, we have $\bar{s}(\bar{r}) \geqq 0$, $(\bar{r} \mid \bar{s}) \geqq 0$. Then by (1.5), $(r \mid s) \geqq 0$. Now, $(r+s \mid r+s)=(r \mid r)+2(r \mid s)+(s \mid s)=1$ or 2. Hence we must have $\lambda(r)=\lambda(s)=1$, $(r \mid s)=0$, $\lambda(r+s)=2$.

(1.9) If $r \in \Sigma$, $\lambda(r)=1$, $r+\bar{r} \in \Sigma$, then $\lambda(r+\bar{r})=1$ and $\overline{r+\bar{r}}=2r+\bar{r}$.

Proof. Since $\lambda(\bar{r})=2$ by (1.4), $\lambda(r+\bar{r})=1$ follows from (1.3). Then $r+\bar{r}=\psi(r+\bar{r})=\bar{r}+2r$.

(1.10)[4] The group W^1 of all $w \in W$ such that $\bar{w}=w$ is of order 16, and consists of $w(\epsilon,\delta,\infty)$, $w(\infty,\epsilon,\delta)$, and $w(\epsilon,\delta,\eta)$, $\epsilon,\delta,\eta=\pm 1$, which are defined by:

$$
\begin{aligned}
&w(\epsilon,\delta,\infty):\\
&\qquad \xi_1 \rightarrow \epsilon\xi_1,\ \xi_2 \rightarrow \epsilon\xi_2,\ \xi_3 \rightarrow \delta\xi_3,\ \xi_4 \rightarrow \delta\xi_4;\\
&w(\infty,\epsilon,\delta):\\
&\qquad \xi_1 \rightarrow \epsilon\xi_3,\ \xi_2 \rightarrow \epsilon\xi_4,\ \xi_3 \rightarrow \delta\xi_1,\ \xi_4 \rightarrow \delta\xi_2;\\
&w(\epsilon,\delta,\eta):\\
&\qquad \xi_1 \rightarrow \tfrac{1}{2}(\epsilon(\xi_1+\xi_2)+\delta(\xi_3+\xi_4)),\\
&\qquad \xi_2 \rightarrow \tfrac{1}{2}(\epsilon(\xi_1-\xi_2)+\delta(\xi_3-\xi_4)),\\
&\qquad \xi_3 \rightarrow \tfrac{1}{2}\eta(\epsilon(\xi_1+\xi_2)-\delta(\xi_3+\xi_4)),\\
&\qquad \xi_4 \rightarrow \tfrac{1}{2}\eta(\epsilon(\xi_1-\xi_2)-\delta(\xi_3-\xi_4)).
\end{aligned}
$$

Proof. Let $\bar{w}=w$. Since $\lambda(w\xi_i)=1$ for all i, we have $w\xi_1=\pm\xi_i$ or $\frac{1}{2}\Sigma\epsilon_i\xi_i$, where $\epsilon_i=\pm 1$. If $w\xi_1=\pm\xi_i$, then the property $(w\xi_1 \mid w\xi_i)=0$ for $i \neq 1$ shows that all $w\xi_i$ are of the form $\pm\xi_i$. Then by using the condition $\psi \circ w=w \circ \psi$ one deduces easily that $w=w(\epsilon,\delta,\infty)$ or $w(\infty,\epsilon,\delta)$ given above. If $w\xi_1$ is of the form $\frac{1}{2}\Sigma\epsilon_i\xi_i$, the same argument as above shows that all $w\xi_i$ have the same form, and from this one can deduce $w=w(\epsilon,\delta,\eta)$.

2. An automorphism of the Chevalley group. The basis elements of the simple Lie algebra of type (F_4) given by Cartan [1, p. 224] can be modified, by multiplying the coefficients ± 1 suitably, so that they satisfy the conditions in Theorem 1 of [2, p. 24]. If, however, the ground field K is of characteristic 2, then Cartan's basis elements can be used directly to define the Chevalley group G of type (F_4) over K (see [4, Section 1] for a definition).

We shall write $x_i(t)$, $x_{ij}(t)$, $x_{ijkl}(t)$ to denote the elements $x_r(t)$, where

---

[4] The group W^1 is actually dihedral.

r are, respectively, the roots given in (1.1). In this notation, we shall write i' instead of $-i$. Thus, for example, $x_{ijk'l'}(t)$ denotes $x_r(t)$, where $r = \frac{1}{2}(\xi_i + \xi_j - \xi_k - \xi_l)$. This way of indicating roots which appear as subscripts will be applied to other symbols also.

By the multiplication table given by Cartan [1, p. 224] and the formulas given by Chevalley [2, p. 26] one obtains the following expressions for the commutators (assuming that K is of characteristic 2):

$$
\begin{aligned}
&(x_i(t), x_j(u)) = 1,\\
&(x_i(t), x_{i'j}(u)) = x_j(tu)x_{ij}(t^2u),\\
&(x_{ij}(t), x_{j'k}(u)) = x_{ik}(tu),\\
(2.1)\qquad &(x_i(t), x_{i'jkl}(u)) = x_{ijkl}(tu),\\
&(x_{ij}(t), x_{i'j'kl}(u)) = x_{ijkl}(tu)x_{kl}(tu^2),\\
&(x_{ijkl}(t), x_{ij'k'l'}(u)) = x_i(tu),\\
&(x_{ijkl}(t), x_{ijk'l'}(u)) = 1,
\end{aligned}
$$

where $(x, y) = x^{-1}y^{-1}xy$, and where all the other commutators of the form $(x_r(t), x_s(u))$ are 1.

It is easy to see that (2.1), above, is equivalent to (2.2)-(2.5), below:

(2.2) If $r, s \in \Sigma$, $r + s \notin \Sigma$, then $(x_r(t), x_s(u)) = 1$.

(2.3) If $r, s, r + s \in \Sigma$, $\lambda(r) = \lambda(s) = 1$, then $(x_r(t), x_s(u)) = x_{r+s}(tu)$ or 1, according as $\lambda(r + s) = 1$ or 2.

(2.4) If $r, s, r + s \in \Sigma$, $\lambda(r) = \lambda(s) = 2$, then $(x_r(t), x_s(u)) = x_{r+s}(tu)$.

(2.5) If $r, s, r + s \in \Sigma$, $\lambda(r) = 1$, $\lambda(s) = 2$, then
$$(x_r(t), x_s(u)) = x_{r+s}(tu)x_{2r+s}(t^2u).$$

Now we shall prove

(2.6) Let $t \to t^\theta$ be an automorphism of the field K.

Then, in (2.1), we can replace $x_r(t)$ by

$$\bar{x}_r(t) = x_{\bar{r}}(t^{\lambda(\bar{r})\theta})$$

without losing the validity of the statements.

Proof. Denote by $(2.n')$, $2 \leqq n \leqq 5$, the statement obtained from $(2.n)$ by the replacement $x_r(t) \to \bar{x}_r(t)$. It suffices to prove that (2.2′)-(2.5′) are valid.

We shall prove (2.2′). If $\bar{r} + \bar{s} \notin \Sigma$, then (2.2′) follows immediately from (2.2). If $\bar{r} + \bar{s} \in \Sigma$, then by (1.8) (using $\bar{r}$, $\bar{s}$ instead of r, s) we have

$\lambda(\bar r) = \lambda(\bar s) = 1$, $\lambda(\bar r + \bar s) = 2$. Hence by (2.3) we have $(x_{\bar r}(t), x_{\bar s}(u)) = 1$ from which (2.2′) follows at once.

We shall prove (2.3′). If $\lambda(r+s) = 1$, then $\bar r + \bar s = \psi(r+s) = \overline{r+s} \in \Sigma$. We have $\lambda(\bar r) = \lambda(\bar s) = 2$. Hence by (2.4),

$$\begin{aligned}(\bar x_r(t), \bar x_s(u)) &= (x_{\bar r}(t^{2\theta}), x_{\bar s}(u^{2\theta}))\\ &= x_{\bar r+\bar s}((tu)^{2\theta}) = \bar x_{r+s}(tu).\end{aligned}$$

If $\lambda(r+s) = 2$, then $\bar r + \bar s = \psi(r+s) = 2(\overline{r+s}) \notin \Sigma$. Hence we obtain $(\bar x_r(t), \bar x_s(u)) = 1$ by (2.2).

We shall prove (2.4′). We have $\lambda(r+s) = 2$ by (1.2). Hence $2\bar r + 2\bar s = \psi(r+s) = 2(\overline{r+s})$, $\bar r + \bar s = \overline{r+s} \in \Sigma$, $\lambda(\bar r + \bar s) = 1$. Then by (2.3) we have

$$(\bar x_r(t), \bar x_s(u)) = (x_{\bar r}(t^{\theta}), x_{\bar s}(u^{\theta})) = x_{\bar r+\bar s}((tu)^{\theta}) = \bar x_{r+s}(tu).$$

We shall prove (2.5′). By (1.3) we have $\lambda(r+s) = 1$, $\lambda(2r+s) = 2$. Hence $2\bar r + 2\bar s = \psi(2r+s) = 2(\overline{2r+s})$. Thus $\bar r + \bar s = \overline{2r+s} \in \Sigma$. Also, $\bar r + 2\bar s = \overline{r+s}$. Hence

$$\begin{aligned}(\bar x_r(t), \bar x_s(u)) = (x_{\bar r}(t^{2\theta}), x_{\bar s}(u^{\theta})) &= (x_{\bar s}(u^{\theta}), x_{\bar r}(t^{2\theta}))^{-1}\\ &= (x_{\bar s+\bar r}(u^{\theta}t^{2\theta})\, x_{2\bar s+\bar r}(u^{2\theta}t^{2\theta}))^{-1}\\ &= (\bar x_{2r+s}(ut^{2})\, \bar x_{r+s}(ut))^{-1}\\ &= \bar x_{r+s}(tu)\, \bar x_{2r+s}(t^{2}u).\end{aligned}$$

Thus the proof of (2.6) is complete.

Using (2.6), above, and proceeding as in [4], one can prove

THEOREM 2.7.[5] *If K is a perfect field of characteristic 2, and if $t \to t^{\theta}$ is an automorphism of K, then the Chevalley group G of type (F_4) over K admits an automorphism $x \to x^{\sigma}$ such that*

$$x_r(t)^{\sigma} = x_{\bar r}(t^{\lambda(\bar r)\theta})$$

for all $r \in \Sigma$ and $t \in K$. We have

$$h(\chi)^{\sigma} = h(\tilde\chi), \qquad \omega_r^{\sigma} = \omega_{\bar r}$$

for all $\chi \in X$ and $r \in \Sigma$, where $\tilde\chi$ is defined by

$$\tilde\chi(r) = \chi(\psi(r))^{\theta} = \chi(\bar r)^{\lambda(r)\theta}.$$

---

[5] After the completion of earlier versions of this paper and [4], the author learned from Tits that the existence of the automorphism σ was already mentioned in [9], p. 282. See also R. Steinberg [8].

3. Invariant elements. From now on we assume that K is a field of characteristic 2 and that K admits an automorphism $t \to t^\theta$ such that

$$2\theta^2 = 1, \tag{3.1}$$

the right hand side being the identity automorphism.[6]

Let G be the Chevalley group of type (F_4) over K and $x \to x^\sigma$ the automorphism of G given in Theorem 2.7. An element $x \in G$ will be said to be *σ-invariant* if $x^\sigma = x$.

We shall order the vector space V (and hence Σ) lexicographically with respect to the coefficients of $\xi_1, \xi_2, \xi_3, \xi_4$. Thus $\xi = \sum c_i \xi_i > 0$ if $\xi \neq 0$ and if the first nonzero number of c_1, c_2, c_3, c_4 is positive.

Let $\mathfrak{U}$ (resp. $\mathfrak{V}$) be the subgroup of G generated by $x_r(t)$ with $r > 0$ (resp. with $r < 0$). Denote by $\mathfrak{U}^1$ (resp. $\mathfrak{V}^1$) the group of σ-invariant elements in $\mathfrak{U}$ (resp. in $\mathfrak{V}$), and by G^1 the group generated by $\mathfrak{U}^1$ and $\mathfrak{V}^1$. Denote by $\mathfrak{H}^1$ the group of all σ-invariant elements in $\mathfrak{H}$, the group of all $h(\chi)$, $\chi \in X$.

First we shall consider $\mathfrak{U}^1$. We shall denote the roots in (1.1) by i, ij, $ijkl$, respectively, writing i' for $-i$. The set of all positive roots in Σ is decomposed into the following 8 disjoint subsets:

$$\begin{array}{lll} & E_1 = \{2, 12', 1, 12\}, & E_5 = \{14, 1234'\}, \\ & E_2 = \{4, 34', 3, 34\}, & E_6 = \{14', 123'4\}, \\ (3.2) & E_3 = \{12'34', 24, 1234, 13\}, & E_7 = \{23, 12'34\}, \\ & E_4 = \{12'3'4, 24', 123'4', 13'\}, & E_8 = \{23', 12'3'4'\}. \end{array}$$

The sets E_1, E_2, E_3, and E_4 are of the form $\{r, \bar{r}, r + \bar{r}, 2r + \bar{r}\}$, while E_5, E_6, E_7, and E_8 are of the form $\{r, \bar{r}\}$, where $r + \bar{r} \notin \Sigma$. Since $\overline{r + \bar{r}} = 2r + \bar{r}$, for $E_1, \cdots, E_4$, one can see easily that, for each E_i, the group generated by $x_s(t)$, $s \in E_i$, $t \in K$ is mapped onto itself by the automorphism σ of G given in (2.7). For $E_i = \{r, \bar{r}\}$, $\lambda(r) = 1$, an element $x_r(t) x_{\bar{r}}(u)$ is σ-invariant if and only if $t = u^\theta$. For $E_i = \{r, \bar{r}, r + \bar{r}, 2r + \bar{r}\}$, let x be an element in the group generated by all $x_s(t)$, $s \in E_i$, $t \in K$. Then

$$\begin{aligned} x^\sigma &= (x_r(t_1) x_{\bar{r}}(t_2) x_{r+\bar{r}}(t_3) x_{2r+\bar{r}}(t_4))^\sigma \\ &= x_{\bar{r}}(t_1^{2\theta}) x_r(t_2^\theta) x_{2r+\bar{r}}(t_3^{2\theta}) x_{r+\bar{r}}(t_4^\theta) \\ &= x_r(t_2^\theta) x_{\bar{r}}(t_1^{2\theta}) x_{r+\bar{r}}(t_1^{2\theta} t_2^{2\theta} + t_4^\theta) x_{2r+\bar{r}}(t_1^{2\theta} t_2^{2\theta} + t_3^{2\theta}) \end{aligned}$$

by (2.5). Hence, by (3.1), $x^\sigma = x$ if and only if $t_1 = t_2^\theta$, $t_3 = t_2^{\theta+1} + t_4^\theta$. Thus, if x is σ-invariant, then x is written uniquely in the form

$$x_r(t^\theta) x_{\bar{r}}(t) x_{r+\bar{r}}(t^{\theta+1}) x_s(u^\theta) x_{\bar{s}}(u),$$

---

[6] It was discovered by Tits that K need not be assumed to be perfect if one considers an endomorphism η, instead of θ, of K such that $\eta^2 = 2$. For the details, see [10].

where $s = r + \bar{r}$, and where $t, u \in K$. The σ-invariant elements obtained from each E_i in the above manner will be called the σ-invariant elements associated with E_i.

Now we shall define the following σ-invariant elements:[7]

$$\begin{aligned}
\alpha_1(t) &= x_4(t^\theta)x_{34'}(t)x_3(t^{\theta+1}),\\
\alpha_2(t) &= x_3(t^\theta)x_{34}(t),\\
\alpha_3(t) &= x_{12'3'4'}(t^\theta)x_{23'}(t),\\
\alpha_4(t) &= x_{12'3'4}(t^\theta)x_{24'}(t)x_{123'4'}(t^{\theta+1}),\\
\alpha_5(t) &= x_2(t^\theta)x_{12'}(t)x_1(t^{\theta+1}),\\
\alpha_6(t) &= x_{12'34'}(t^\theta)x_{24}(t)_{1234}(t^{\theta+1}),\\
\alpha_7(t) &= x_{12'34}(t^\theta)x_{23}(t),\\
\alpha_8(t) &= x_{123'4'}(t^\theta)x_{13'}(t),\\
\alpha_9(t) &= x_{123'4}(t^\theta)x_{14'}(t),\\
\alpha_{10}(t) &= x_{1234'}(t^\theta)x_{14}(t),\\
\alpha_{11}(t) &= x_{1234}(t^\theta)x_{13}(t),\\
\alpha_{12}(t) &= x_1(t^\theta)x_{12}(t).
\end{aligned}$$

We shall denote by R_i the set of roots appearing in the above expression of $\alpha_i(t)$, and by $\min(R_i)$ the minimum root in R_i. Thus, for instance, $R_1 = \{\xi_4, \xi_3 - \xi_4, \xi_3\}$, and $\min(R_1) = \xi_4$. We can verify from the above that

$$(3.3) \qquad \min(R_1) < \min(R_2) < \cdots < \min(R_{12}).$$

We shall prove

(3.4) If an element

$$x = x_{r_1}(t_1)x_{r_2}(t_2)\cdots x_{r_m}(t_m)$$

where all $r_i > 0$, is σ-invariant, then x can be written uniquely as

$$x = \alpha_1(u_1)\alpha_2(u_2)\cdots\alpha_{12}(u_{12})$$

with $u_i \in K$. For any i such that $u_i \neq 0$, any root in R_i is a linear combination, with integral coefficients $\geqq 0$, of the roots $r_1, r_2, \cdots, r_m$.

Proof. By (1.2) of [4], we can assume without loss of generality that $r_1 < r_2 < \cdots < r_m$, and that all $t_i \neq 0$. Since x is σ-invariant,

$$x = x_{\bar{r}_1}(\bar{t}_1)x_{\bar{r}_2}(\bar{t}_2)\cdots x_{\bar{r}_m}(\bar{t}_m),$$

where, for all i,

$$(3.5) \qquad \bar{t}_i = t_i^{\lambda(\bar{r}_i)\theta}.$$

---

[7] For an idea of avoiding the use of the elements $\alpha_1(t), \cdots, \alpha_{12}(t)$, see [10, section 2]. The conjecture stated there was proved by Tits himself.

Let $\bar{r}_i$ be the minimum root in the set $\{\bar{r}_1, \bar{r}_2, \cdots, \bar{r}_m\}$. Then clearly x can be written in the form

$$x = x_{\bar{r}_i}(\bar{t}_i)x',$$

where x' is a product of elements $x_r(t)$ with $r > \bar{r}_i$. Then by Lemma 6 of [2, p. 39] we have

$$(3.6) \qquad r_1 = \bar{r}_i, \qquad t_1 = \bar{t}_i.$$

We can clearly write

$$x = x_{r_1}(t_1)x_{r_i}(t_i)x'',$$

where x'' is a product of the elements $x_r(t)$ such that r is a linear combination, with integral coefficients $\geqq 0$, of the roots $r_1, r_2, \cdots, r_m$, and such that $r > r_1$. Now (3.5) and (3.6) show that there exists an $\alpha_k(v)$ such that $x = \alpha_k(v)y$, where y is a product of the elements $x_r(t)$ such that r is a linear combination, with integral coefficients $\geqq 0$, of the roots $r_1, \cdots, r_m$ and such that $r > r_1$. Now we can proceed by induction on r_1, which is clearly uniquely determined by x. If r_1 is sufficiently large, then (3.4) is clear. Hence by applying the induction assumption to y, we have

$$y = \alpha_{k_1}(u_1) \cdots \alpha_{k_n}(u_n),$$

where $k_1 < \cdots < k_n$. Clearly $k < k_1$ (if $u_1 \neq 0$). Hence we conclude that x can be written in the desired form.

The uniqueness part follows easily from Lemma 6 of [2, p. 39] and (3.3), above. The rest of (3.4) is also clear.

(3.7) For any i, j, the commutator $(\alpha_i(t), \alpha_j(u))$ can be written as

$$(\alpha_i(t), \alpha_j(u)) = \alpha_k(v_k)\alpha_{k+1}(v_{k+1}) \cdots \alpha_{12}(v_{12}),$$

where $\min(R_k) \geqq \min(R_i) + \min(R_j)$.

Proof. By (1.2) of [4] one can see easily that the commutator $(\alpha_i(t), \alpha_j(u))$ can be written as $\prod x_r(t_r)$, where $r \geqq \min(R_i) + \min(R_j)$. Hence (3.7) follows immediately from (3.4).

Denote by $\mathfrak{U}^i$ the group generated by $\alpha_i(t), \alpha_{i+1}(t), \cdots, \alpha_{12}(t)$, $t \in K$. Note that, by (3.4), the new definition for $\mathfrak{U}^1$ is equivalent to the old one given at the beginning of this section. Also, set $\mathfrak{U}^{13} = \{1\}$. Then from (3.7) one can derive

(3.8) Let $1 \leqq i \leqq 12$. If $x \in \mathfrak{U}^1$, $y \in \mathfrak{U}^i$, then $(x, y) \in \mathfrak{U}^{i+1}$.

For any element $w \in W$, define $\mathfrak{U}_w$ to be the subgroup of $\mathfrak{U}$ generated by all $x_r(t)$ such that $w(r) < 0$. If $w \in W^1$ (see (1.10)), and if $w(r) < 0$

for some $r \in R_i$, then by (1.7) we have $w(r) < 0$ for all $r \in R_i$. In this case, we shall write $w(R_i) < 0$. We have

(3.9) If $w \in W^1$, then every element in $\mathfrak{U}_w \cap \mathfrak{U}^1$ is written uniquely as $x = \alpha_1(t_1)\alpha_2(t_2) \cdots \alpha_{12}(t_{12})$, where $t_i = 0$ unless $w(R_i) < 0$.

Proof. This also follows immediately from (3.4).

Now we shall consider the group $\mathfrak{B}^1$. By considering negative roots instead of positive roots, one obtains, as generators of $\mathfrak{B}^1$, the elements $\alpha'_1(t), \alpha'_2(t), \cdots, \alpha'_{12}(t)$, where $\alpha'_i(t)$ is the element obtained by replacing every x_r by x_{-r} in the expression of $\alpha_i(t)$. Thus, for instance,

$$\alpha'_1(t) = x_{4'}(t^{\theta})x_{3'4}(t)x_{3'}(t^{\theta+1}).$$

We shall prove

(3.10) Let $E_i = \{r, \bar{r}, r + r, 2r + \bar{r}\}$ be any one of E_1, E_2, E_3, E_4 given in (3.2), and let

$$\alpha_j(t) = x_r(t^{\theta})x_{\bar{r}}(t)\,x_{r+\bar{r}}(t^{\theta+1}),$$
$$\alpha_k(t) = x_{r+\bar{r}}(t^{\theta})\,x_{2r+\bar{r}}(t)$$

be the σ-invariant elements associated with E_i. If $t \neq 0$, then

$$\alpha'_k(t) = \alpha_j(t^{1-2\theta})^{-1}h(\chi)\,\omega_{\bar{r}}\,\omega_{2r+\bar{r}}\alpha_j(t^{1-2\theta}),$$

where χ is given by

$$\chi = \chi_{\bar{r},t^{1-2\theta}}\chi_{2r+\bar{r},t^{-1}}.$$

Proof. We have

$$\alpha'_k(t) = x_{-(r+\bar{r})}(t^{\theta})\,x_{-(2r+\bar{r})}(t).$$

By (6.2) in [4], we have

$$x_{-(2r+\bar{r})}(t) = x_{2r+\bar{r}}(t^{-1})\,h(\chi_1)\,\omega_{2r+\bar{r}}x_{2r+\bar{r}}(t^{-1}),$$

where

$$\chi_1 = \chi_{2r+\bar{r},t^{-1}}.$$

Since, by (2.5),

$$\begin{aligned} &x_{-(r+\bar{r})}(t^{\theta})x_{2r+\bar{r}}(t^{-1})\,x_{-(r+\bar{r})}(t^{\theta}) \\ &\qquad = x_{2r+\bar{r}}(t^{-1})x_r(t^{\theta-1})\,x_{-\bar{r}}(t^{2\theta-1}) \\ &\qquad = x_{2r+\bar{r}}(t^{-1})x_r(t^{\theta-1})x_{\bar{r}}(t^{1-2\theta})\,h(\chi_2)\,\omega_{\bar{r}}\,x_{\bar{r}}(t^{1-2\theta}), \end{aligned}$$

where

$$\chi_2 = \chi_{\bar{r},t^{1-2\theta}},$$

we have

$$\begin{aligned}\alpha'_k(t) &= x_{2r+\bar r}(t^{-1})\,x_r(t^{\theta-1})\,x_{\bar r}(t^{1-2\theta})\,h(\chi_2)\,\omega_{\bar r}\,x_{\bar r}(t^{1-2\theta})\\ &\quad\cdot x_{-(r+\bar r)}(t^{\theta})\,h(\chi_1)\,\omega_{2r+\bar r}\,x_{2r+\bar r}(t^{-1})\\ &= x_{2r+\bar r}(t^{-1})\,x_r(t^{\theta-1})\,x_{\bar r}(t^{1-2\theta})\,h(\chi_2)\,h(\chi_1\circ w_{\bar r})\,\omega_{\bar r}\\ &\quad\cdot x_{\bar r}(\chi_1(\bar r)^{-1}t^{1-2\theta})\,x_{-(r+\bar r)}(\chi_1(r+\bar r)\,t^{\theta})\,\omega_{2r+\bar r}\,x_{2r+\bar r}(t^{-1}).\end{aligned}$$

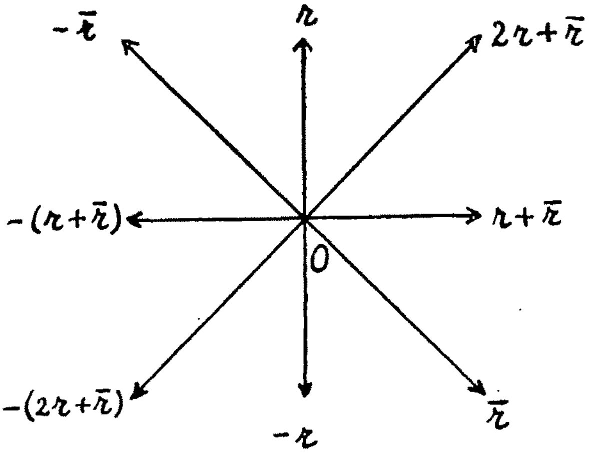

FIGURE 1.

We have

$$\chi_1(\bar r) = 1,\ \chi_1(r+\bar r) = t^{-1},\ \text{and}\ \chi_1\circ w_{\bar r} = \chi_1,$$

since $w_{\bar r}(2r+\bar r) = 2r+\bar r$. Hence

$$\begin{aligned}\alpha'_k(t) &= x_{2r+\bar r}(t^{-1})\,x_r(t^{\theta-1})\,x_{\bar r}(t^{1-2\theta})\,h(\chi)\,\omega_{\bar r}\,\omega_{2r+\bar r}\\ &\quad\cdot x_{\bar r}(t^{1-2\theta})\,x_r(t^{\theta-1})\,x_{2r+\bar r}(t^{-1}),\end{aligned}$$

where χ is as given in (3.10). From this and (2.5) one can derive the desired result easily. Thus (3.10) is proved.

Set $t=1$ in (3.10). Then $h(\chi)=1$. Hence we have $\omega_{\bar r}\omega_{2r+\bar r}\in G^1$. Hence by setting $E_i = E_1, E_2, E_3, E_4$ we obtain

(3.11) G^1 contain the elements $\omega_{12'}\omega_{12}$, $\omega_{34'}\omega_{34}$, $\omega_{24}\omega_{13}$, $\omega_{24'}\omega_{13'}$.

Now, any one of E_5, E_6, E_7, E_8 is of the form $E_i = \{r, \bar r\}$, where $r+\bar r\notin\Sigma$, $r-\bar r\notin\Sigma$. Hence if $\alpha_j(t) = x_r(t\ )x_{\bar r}(t)$ (we assume that $\lambda(r)=1$) are the σ-invariant elements associated with E_i, then

$$\omega_r\omega_{\bar r} = \alpha_j(1)\,\alpha'_j(1)\,\alpha_j(1)\in G^1.$$

Hence, by setting $E_i = E_5, E_6, E_7, E_8$, we obtain

(3.12) G^1 contains $\omega_{1234'}\omega_{14}$, $\omega_{123'4}\omega_{14'}$, $\omega_{12'34}\omega_{23}$, $\omega_{12'3'4'}\omega_{23'}$.

It can be easily seen that the elements $w_{12'}w_{12}$, $w_{34'}w_{34}$, $w_{24}w_{13}$, $w_{24'}w_{13'}$, $w_{1234'}w_{14}$, $w_{123'4}w_{14'}$, $w_{12'34}w_{23}$, and $w_{12'3'4'}w_{23'}$ generate the group W^1 defined in (1.10). Hence (3.11) and (3.12) yield

(3.13) For every $w \in W^1$ we can take $\omega(w)$ in G^1 so that $\omega(w)^\sigma = \omega(w)$.

In what follows we shall take $\omega(w)$ in G^1 for all $w \in W^1$, $\omega(1) = 1$.

Now we shall consider the group $\mathfrak{H}^1$ of σ-invariant elements in $\mathfrak{H}$. As in Theorem 4.8 of [4] we have

$$h(\chi)^\sigma = h(\bar{\chi}),$$

where $\bar{\chi}$ is defined by

$$\bar{\chi}(r) = \chi(\psi(r))^\theta = \chi(\bar{r})^{\lambda(r)\theta}.$$

Hence we can deduce easily

(3.14) $h(\chi) \in \mathfrak{H}^1$ if and only if

$$\chi(\xi_2) = \chi(\xi_1)^{2\theta-1}, \ \chi(\xi_4) = \chi(\xi_3)^{2\theta-1}.$$

If $E_i = \{r, \bar{r}, r + \bar{r}, 2r + \bar{r}\}$ is any one of E_1, E_2, E_3, E_4, then by (3.11) we have $h(\chi) \in G^1$, where χ is given in (3.10). A simple calculation shows that if $E_i = E_1$, then

$$\chi(\xi_1) = t^{-2\theta}, \qquad \chi(\xi_2) = t^{2\theta-2}, \quad \chi(\xi_3) = \chi(\xi_4) = 1.$$

On the other hand, if $E_i = E_2$, then

$$\chi(\xi_1) = \chi(\xi_2) = 1, \qquad \chi(\xi_3) = t^{-2\theta}, \qquad \chi(\xi_4) = t^{2\theta-2}.$$

Since t is an arbitrary element in K^*, we have by (3.14)

$$\mathfrak{H}^1 \subseteq G^1 \tag{3.15}$$

Now we shall prove

(3.16) G^1 is the group of all σ-invariant elements in G. Any element $x \in G^1$ is written uniquely as $x = uh(\chi)\omega(w)u'$, where $u \in \mathfrak{U}^1$, $h(\chi) \in \mathfrak{H}^1$, $w \in W^1$, $u' \in \mathfrak{U}_w \cap \mathfrak{U}^1$.

Proof. By (1.13) of [4], any $x \in G$ can be written uniquely as $x = uh(\chi)\omega(w)u'$, where $u \in \mathfrak{U}$, $h(\chi) \in \mathfrak{H}$, $w \in W$, $u' \in \mathfrak{U}_w$. Then

$$x^\sigma = u^\sigma h(\bar{\chi})\omega(w)^\sigma u'^\sigma.$$

Proceeding as in the proof of (5.16) of [4], we have $\zeta(\omega(w)^\sigma) = \bar{w}$ and $(\mathfrak{U}_w)^\sigma = \mathfrak{U}_{\bar{w}}$. Hence $\omega(w)^\sigma = h(\chi_1)\omega(\bar{w})$ and $u'^\sigma \in \mathfrak{U}_w$. Therefore, if $x^\sigma = x$, then by the uniqueness we have $u^{\sigma}=u$, $\chi=\bar{\chi}\chi_1$, $\bar{w}=w$, $u'^{\sigma}=u'$. Hence $\chi_1=1$, $\chi=\bar{\chi}$. Now (3.16) follows from (3.13) and (3.15).

4. The center of $\mathfrak{U}^1$. As a preparation for the proof of the simplicity of G^1, we shall prove here that the center of $\mathfrak{U}^1$ consists of the elements $\alpha_{12}(t)$, $t\in K$. In this section, we do *not* assume that K has more than 2 elements, although we will prove, in the next section, the simplicity of G^1 under that assumption.

Let the groups $\mathfrak{U}^1, \mathfrak{U}^2, \cdots, \mathfrak{U}^{12}$ be as in the preceding section. By (3.8), $\mathfrak{U}^i$ is clearly a normal subgroup of $\mathfrak{U}^1$.

All the expressions for the commutators

$$(\alpha_i(t),\alpha_j(u))=\alpha_i(t)^{-1}\alpha_j(u)^{-1}\alpha_i(t)\alpha_j(u)$$

used throughout this section can be derived easily from (2.2)-(2.5).

Now, let

$$c=\alpha_1(t_1)\alpha_2(t_2)\cdots\alpha_{12}(t_{12})$$

be an element in the center of $\mathfrak{U}^1$.

We shall first prove $t_1=t_4=0$. We have

$$(\alpha_i(t),\alpha_{10}(u))=1 \qquad (i\neq 1,4) \tag{4.1}$$

Note that (4.1) for $i\geq 8$ follows from (3.7). Also

$$(\alpha_1(t),\alpha_{10}(u))=\alpha_{11}(tu). \tag{4.2}$$

$$(\alpha_4(t),\alpha_{10}(u))=\alpha_{12}(tu). \tag{4.3}$$

Hence $\alpha_{10}(u)^{-1}c\alpha_{10}(u)$ is equal to

$$\alpha_1(t_1)\alpha_{11}(t_1u)\alpha_2(t_2)\alpha_3(t_3)\alpha_4(t_4)\alpha_{12}(t_4u)\alpha_5(t_5)\cdots\alpha_{12}(t_{12}).$$

Equating this to c, and noting that $\alpha_{12}(t)$ is in the center of $\mathfrak{U}^1$, we have $\alpha_{11}(t_1u)\alpha_{12}(t_4u)=1$. Hence $t_1u=t_4u=0$ for all $u\in K$. Hence we obtain $t_1=t_4=0$.

We shall prove $t_3=0$. We have

$$(\alpha_i(t),\alpha_2(u))=1 \qquad (i=2,5,6) \tag{4.4}$$

$$\begin{aligned}(\alpha_3(t),\alpha_2(u))=&\,\alpha_5(t^{2\theta}u)\alpha_6(tu)\alpha_7(tu^{2\theta})\alpha_8(t^{2\theta+1}u)\\ &\cdot\alpha_9(t^{2\theta+1}u^{2\theta})\alpha_{10}(t^{2\theta+1}u^2)\alpha_{12}(t^{2\theta+2}u^{2\theta+1}).\end{aligned} \tag{4.5}$$

By (4.4), (4.5), above, we can easily compare c (mod $\mathfrak{U}^6$) and $\alpha_2(u)^{-1}c\alpha_2(u)$ (mod $\mathfrak{U}^6$), and obtain $t_3=0$.

We shall prove $t_2 = 0$. By (4.4) and (4.5) we have

$$(\alpha_2(t), \alpha_3(u)) \equiv \alpha_5(tu^{2\theta})^{-1} \pmod{\mathfrak{U}^6}.$$

Combining this with

$$(\alpha_5(t), \alpha_3(u)) = \alpha_8(tu) \tag{4.6}$$

we can derive easily $t_2 = 0$.

For the determination of $t_5, t_6, \cdots$, we need

$$(\alpha_6(t), \alpha_3(u)) = \alpha_8(tu^{2\theta})\alpha_9(t^{2\theta}u)\alpha_{12}(t^{2\theta+1}u), \tag{4.7}$$

$$(\alpha_7(t), \alpha_3(u)) = \alpha_9(tu^{2\theta})\alpha_{10}(t^{2\theta}u), \tag{4.8}$$

$$(\alpha_i(t), \alpha_3(u)) = 1 \quad (i = 8, 9, 10, 12), \tag{4.9}$$

$$(\alpha_{11}(t), \alpha_3(u)) = \alpha_{12}(tu). \tag{4.10}$$

By (4.7)-(4.10), above, $\alpha_3(u)^{-1}c\alpha_3(u)$ is equal to

$$\alpha_5(t_5)\alpha_8(t_5u)\alpha_6(t_6)\alpha_8(t_6u^{2\theta})\alpha_9(t_6{}^{2\theta}u)\alpha_{12}(t_6{}^{2\theta+1}u)\alpha_7(t_7)\alpha_9(t_7u^{2\theta})$$
$$\cdot\alpha_{10}(t_7{}^{2\theta}u)\alpha_8(t_8)\alpha_9(t_9)\alpha_{10}(t_{10})\alpha_{11}(t_{11})\alpha_{12}(t_{11}u)\alpha_{12}(t_{12}).$$

Equating this with c and simplifying the relation by

$$\begin{aligned}(\alpha_8(t), \alpha_6(u)) = (\alpha_9(t), \alpha_8(u)) = (\alpha_9(t), \alpha_7(u))\\ = (\alpha_{10}(t), \alpha_8(u)) = (\alpha_{10}(t), \alpha_9(u)) = 1,\end{aligned} \tag{4.11}$$

$$(\alpha_8(t), \alpha_7(u)) = \alpha_{12}(tu) \tag{4.12}$$

we obtain

$$t_5u + t_6u^{2\theta} = 0, \quad t_6{}^{2\theta}u + t_7u^{2\theta} = 0, \quad t_7{}^{2\theta}u = 0,$$
$$(t_5u + t_6u^{2\theta})t_7 + t_6{}^{2\theta+1}u + t_{11}u = 0$$

for all $u \in K$. Hence we have $t_5 = t_6 = t_7 = t_{11} = 0$.

Now, simplifying the relation $\alpha_7(u)^{-1}c\alpha_7(u) = c$ by (4.11), (4.12), and $(\alpha_{10}(t), \alpha_7(u)) = (\alpha_{11}(t), \alpha_7(u)) = 1$, we obtain $t_8 = 0$.

Similarly, simplifying the relation $\alpha_6(u)^{-1}c\alpha_6(u) = c$ by $(\alpha_{10}(t), \alpha_6(u)) = (\alpha_{11}(t), \alpha_6(u)) = 1$ and

$$(\alpha_9(t), \alpha_6(u)) = \alpha_{12}(tu), \tag{4.13}$$

we obtain $t_9 = 0$.

Finally, simplifying the relation $\alpha_4(u)^{-1}c\alpha_4(u) = c$ by (4.3) and $(\alpha_{11}(t), \alpha_4(u)) = 1$, we obtain $t_{10} = 0$. Thus we have proved

THEOREM 4.14. *The center of* $\mathfrak{U}^1$ *consists of the elements* $\alpha_{12}(t)$, $t \in K$.

5. The simplicity of G^1. We shall prove the simplicity of G^1 under the assumption that K contains more than 2 elements. If K contains only 2 elements, then G^1 is of order $2^{12} \cdot 3^3 \cdot 5^2 \cdot 13$ (see Section 6). The author does not know the composition factors of this group.

First we shall prove a lemma which requires the above mentioned assumption.

(5.1) If $w \in W^1$, $w \neq 1$, then there exists an $h \in \mathfrak{H}^1$ such that $\omega(w)h \neq h\omega(w)$.

Proof. Since $\omega(w)h(\chi)\omega(w)^{-1} = h(\chi')$, where χ' is defined by $\chi'(r) = \chi(w^{-1}(r))$, it suffices to derive a contradiction by assuming that $\chi(wr) = \chi(r)$ for all $r \in \Sigma$ and all χ such that $h(\chi) \in \mathfrak{H}^1$.

If $w = w(\epsilon, \delta, \infty)$ or $w(\infty, \epsilon, \delta)$ (see (1.10)), then $w \neq 1$ implies that $w(\xi_1) = -\xi_1$ or $w(\xi_1) = \pm\xi_3$. Then $\chi(\xi_1)^2 = 1$ or $\chi(\xi_1) = \chi(\pm\xi_3)$. This is clearly impossible, since, by (3.14), $\chi(\xi_1)$ and $\chi(\xi_3)$ can be regarded as arbitrary elements in K^*, and since K contains more than 2 elements.

If $w = w(\epsilon, \delta, \eta)$, then from $\chi(w\xi_1) = \chi(\xi_1)$ and $\chi(w\xi_3) = \chi(\xi_3)$ one derives easily $\chi(\xi_1 + \xi_2)^{\epsilon} = \chi(\xi_1)\chi(\xi_3)^{\eta}$ which is also clearly impossible by the reason stated above. Thus (5.1) is proved.

Now we shall proceed to prove the simplicity of G^1. Let $H \neq \{1\}$ be a normal subgroup of G^1. By (3.16), H contains an element $x = uh\omega(w) \neq 1$ with $u \in \mathfrak{U}^1$, $h \in \mathfrak{H}^1$, and $w \in W^1$. If $w \neq 1$, then, by (5.1), there exists $h_1 \in \mathfrak{H}^1$ such that $\omega(w)h_1 \neq h_1\omega(w)$. We have $1 \neq xh_1x^{-1}h_1^{-1} \in \mathfrak{U}^1\mathfrak{H}^1 \cap H$. Thus we have proved that H contains an element $x = uh \neq 1$, where $u \in \mathfrak{U}^1$, $h \in \mathfrak{H}^1$. Suppose $h = h(\chi) \neq 1$. Then H contains, for any $t \in K^*$,

$$y = x\alpha_{12}(t)x^{-1}\alpha_{12}(t)^{-1} = \alpha_{12}((\chi(\xi_1 + \xi_2) - 1)t)$$

and

$$y' = x\alpha_2(t)x^{-1}\alpha_2(t)^{-1} = \alpha_2((\chi(\xi_3 + \xi_4) - 1)t)y'',$$

where $y'' \in \mathfrak{U}^3$, the group generated by the elements $\alpha_3(t), \cdots, \alpha_{12}(t)$, $t \in K$. Hence if $y = y' = 1$ for all $t \in K^*$, then by (3.4) we would have $\chi(\xi_1 + \xi_2) = \chi(\xi_3 + \xi_4) = 1$, and hence by (3.14), $\chi = 1$, a contradiction. Thus we have proved that H contains an element $x \neq 1$ in $\mathfrak{U}^1$. Suppose x is not in the center of $\mathfrak{U}^1$. Then there exists $y \in \mathfrak{U}^1$ such that the commutator $(x, y) \neq 1$. If $x \in \mathfrak{U}^i$, then, by (3.8), $(x, y) \in \mathfrak{U}^{i+1}$. Hence H must contain an element $\neq 1$ in the center of $\mathfrak{U}^1$. By (4.16), H contains $\alpha_{12}(t)$ with some $t \neq 0$.

Then by considering $h(\chi)\alpha_{12}(t)h(\chi)^{-1}$ we see easily that H contains $\alpha_{12}(t)$ for all $t \in K$.

Since G^1 contains $\omega_0 = \omega(w(-1,-1,\infty))$ by (3.13), H also contains $\alpha'_{12}(t) = \omega_0\alpha_{12}(t)\omega_0^{-1}$ for all $t \in K$. Now, setting $r = \xi_2$ in (3.10), we have $\alpha_k = \alpha_{12}$. Hence by (3.10), H contains $h(\chi)\omega_{12'}\omega_{12}$, where χ is defined in (3.10) with $r = \xi_2$. If $t = 1$, then $h(\chi) = 1$. Hence H contains $\omega_{12'}\omega_{12}$ and $h(\chi)$ for all $t \in K^*$. We have

$$\chi(\xi_1) = t^{-2\theta}, \quad \chi(\xi_2) = t^{2\theta-2}, \quad \chi(\xi_3) = \chi(\xi_4) = 1. \tag{5.2}$$

Hence, for any $u \in K$ and $t \in K^*$, H contains

$$\begin{aligned}\alpha_5(u)h(\chi)\alpha_5(u)^{-1}h(\chi)^{-1} &= \alpha_5(u)\alpha_5(t^{2-4\theta}u)^{-1}\\ &= \alpha_5(u + t^{2-4\theta}u)\alpha_{12}(u^{2\theta+1}(t^{2\theta-4} + t^{-2\theta-2}))\end{aligned}$$

Therefore H contains $\alpha_5(u + t^{2\theta-4}u)$ for all $u \in K$ and $t \in K^*$. Since $1 + t^{2\theta-4} = 0$ implies $t = 1$, and since K has more than 2 elements, it follows that H contains $\alpha_5(t)$ for all $t \in K$. Thus we have shown that H contains, for all t and u in K, the elements $\alpha_5(t)\alpha_{12}(u)$, which are precisely the σ-invariant elements associated with the set E_1 given in (3.2).

Since $w(\infty,1,1)$, $w(1,1,1)$, $w(1,-1,1)$ map E_1 onto E_2, E_3, E_4, respectively, it follows from (1.6) of [4] and (3.13) that H contains all the σ-invariant elements associated with E_2, E_3, E_4 also.

Now we shall turn to the σ-invariant elements associated with the sets $E_5, \cdots, E_8$. We have already seen in the above that H contains $h(\chi)$ with χ defined in (5.2). Hence H contains, for any $u \in K$ and $t \in K^*$,

$$h(\chi)\alpha_{10}(u)h(\chi)^{-1}\alpha_{10}(u)^{-1} = \alpha_{10}(u + t^{-2\theta}u).$$

Since $1 + t^{-2\theta} = 0$ implies $t = 1$ and since K contains more than 2 elements, it follows from the above that H contains $\alpha_{10}(t)$ for all $t \in K$. Now, $\alpha_{10}(t)$, $t \in K$, are exactly the σ-invariant elements associated with the set E_5. Since $w(1,-1,\infty)$, $w(\infty,1,1)$, $w(-1,1,\infty)$ map E_5 onto E_6, E_7, E_8, respectively, we conclude, as above, that H contains all the σ-invariant elements associated with the sets E_6, E_7, and E_8.

Thus H contains all the σ-invariant elements associated with $E_1, \cdots, E_8$. This implies that H contains $\alpha_1(t), \cdots, \alpha_{12}(t)$, for all $t \in K$, since any $\alpha_i(t)$ is associated with some E_j. Since G^1 contains $\omega_0 = \omega(w(-1,-1,\infty))$, it follows that H contains $\alpha'_i(t) = \omega_0\alpha_i(t)\omega_0^{-1}$ for all $i = 1, \cdots, 12$, and $t \in K$. Therefore we have $H = G^1$. Thus we have proved

THEOREM 5.3. *If K possesses more than 2 elements, then the group G^1 is simple.*

6. The finite groups.

Let K be a finite field of $q = 2^{2n+1}$ elements, where $n = 0, 1, 2, \cdots$. Then the automorphism $t \to t^\theta$ defined by $t^\theta = t^m$, where $m = 2^n$, satisfies $2\theta^2 = 1$. Hence the group G^1 can be defined over K. We shall compute the order of G^1. By (3.16), G^1 can be partitioned into the 16 subsets:

$$\mathfrak{U}^1 \mathfrak{H}^1 \omega(w)(\mathfrak{U}_w \cap \mathfrak{U}^1),$$

where w runs over the 16 elements of W^1. The order of $\mathfrak{U}^1$ is, by (3.4), q^{12}, and the order of $\mathfrak{H}^1$ is, by (3.14), $(q-1)^2$. The order of $\mathfrak{U}_w \cap \mathfrak{U}^1$ is, by (3.9), $q^{n(w)}$, where $n(w)$ denotes the number of indices $i = 1, \cdots, 12$, such that $w(R_i) < 0$. Hence the order of G^1 is

$$q^{12}(q-1)^2 \sum q^{n(w)}, \tag{6.1}$$

where the sum runs over all $w \in W^1$.

We shall compute the numbers $n(w)$, $w \in W^1$. Note first that if $\alpha_i(t)$ and $\alpha_j(t)$ are associated with the same set E_k, then $w(E_i) < 0$ if and only if $w(E_j) < 0$. In fact, it can be easily seen that, if $w(r) < 0$ for some $r \in E_k$, then $w(r) < 0$ for all $r \in E_k$. For $w \in W^1$, define $\nu(w; E_k) = 1$ or -1 according as $w(r) > 0$ for all $r \in E_k$ or not. Then we have

$$n(w) = \sum_{1 \leq k \leq 4} (1 - \nu(w; E_k)) + \tfrac{1}{2} \sum_{5 \leq k \leq 8} (1 - \nu(w; E_k)). \tag{6.2}$$

The numbers $\nu(w; E_k)$ can be computed easily by (1.10) and (3.2). We have

The table of $\nu(w; E_k)$

	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8
$w(\epsilon, \delta, \infty)$	ϵ	δ	ϵ	ϵ	ϵ	ϵ	ϵ	ϵ
$w(\infty, \epsilon, \delta)$	ϵ	δ	δ	$-\delta$	δ	$-\delta$	ϵ	$-\epsilon$
$w(\epsilon, \delta, 1)$	ϵ	ϵ	ϵ	δ	ϵ	ϵ	ϵ	$-\epsilon$
$w(\epsilon, \delta, -1)$	ϵ	$-\epsilon$	δ	ϵ	ϵ	ϵ	$-\epsilon$	ϵ

Hence by (6.2) we have

$$\begin{aligned} n(w(\epsilon, \delta, \infty)) &= 6 - 5\epsilon - \delta = 0, 2, 10, 12, \\ n(w(\infty, \epsilon, \delta)) &= 6 - \epsilon - \delta = 4, 6, 6, 8, \\ n(w(\epsilon, \delta, 1)) &= 6 - 4\epsilon - \delta = 1, 3, 9, 11, \\ n(w(\epsilon, \delta, -1)) &= 6 - 2\epsilon - \delta = 3, 5, 7, 9. \end{aligned}$$

Therefore $\sum q^{n(w)}$ is equal to

$$1+q+q^2+2q^3+q^4+q^5+2q^6+q^7+q^8+2q^9+q^{10}+q^{11}+q^{12}$$
$$=(q+1)(q^2+1)(q^3+1)(q^6+1).$$

Hence by (6.1) we have

THEOREM 6.3. *If K is a finite field of $q=2^{2n+1}$ elements, where $n=0,1,2,\cdots$, then the order of G^1 is given by*

$$q^{12}(q-1)(q^3+1)(q^4-1)(q^6+1).$$

7. Automorphisms of G^1. If $t \to t'$ is an automorphism of the field K which commutes with θ, then there exists an automorphism ρ of G^1 such that $\alpha_i(t) \to \alpha_i(t')$, $\alpha'_i(t) \to \alpha'_i(t')$ for all $t \in K$ and i. We shall call ρ the automorphism of G^1 induced by the automorphism $t \to t'$ of K. We shall prove

THEOREM 7.1. *If K is a finite[8] field possessing more than 2 elements, then every automorphism ρ of the group G^1 can be written uniquely in the form $\rho=\rho_1\rho_2$, where ρ_1 is an automorphism induced by an automorphism of K, and where ρ_2 is an inner automorphism of G^1.*

Proof. Arguing as in the proof of Theorem 9.1 of [4], we see that we can assume (7.2)-(7.5), below:

$$(\mathfrak{U}^1)^\rho=\mathfrak{U}^1, \tag{7.2}$$

$$\alpha_{12}(t)^\rho=\alpha_{12}(t) \quad \text{for all } t \in K, \tag{7.3}$$

$$h(\chi)^\rho=h(\chi) \quad \text{for all } h(\chi) \in \mathfrak{H}^1, \tag{7.4}$$

$$\omega_0{}^\rho=h(\chi_0)\omega_0 \quad \text{where } \omega_0=\omega(w(-1,-1,\infty)). \tag{7.5}$$

Define the roots $r_1, r_2, \cdots, r_{12}$ by setting $r_i=\bar{r}$ if $\alpha_i(t)=x_r(t^\theta)x_{\bar{r}}(t)$ or if $\alpha_i(t)=x_r(t^\theta)x_{\bar{r}}(t)x_{r+\bar{r}}(t^{\theta+1})$. Then the roots $r_1,\cdots,r_{12}$ are respectively,

$$34', 34, 23', 24', 12', 24, 23, 13', 14', 14, 13, 12,$$

where ij and ij' denote $\xi_i+\xi_j$ and $\xi_i-\xi_j$, respectively. From the definition of r_i we have

$$h(\chi)\alpha_i(t)h(\chi)^{-1}=\alpha_i(\chi(r_i)t) \tag{7.6}$$

---

[8] J. Tits remarks that the finiteness assumption seems to be dispensed with if one uses the geometric interpretation of the group G^1 given in [10].

for all $h(\chi) \in \mathfrak{H}^1$ and $t \in K$. Now fix an i, and set

$$\alpha_i(t)^\rho = \alpha_1(t^{(1)})\alpha_2(t^{(2)}) \cdots \alpha_{12}(t^{(12)}).$$

Then by (7.4) and (7.6) we have

$$(\chi(r_i)t)^{(j)} = \chi(r_j)t^{(j)} \tag{7.7}$$

Hence if for the root r_j, there exists $h(\chi) \in \mathfrak{H}^1$ such that $\chi(r_i) = 1$ and $\chi(r_j) \neq 1$, then we have $t^{(j)} = 0$ for all $t \in K$. Using this, (3.13), and the assumption that K has more than 2 elements, we can deduce (7.8)-(7.10), below:

(7.8) If $i \neq 1, 2, 5$, then $\alpha_i(t)^\rho = \alpha_i(c_i t)$, where c_i is a constant in K.

(7.9) Both $\alpha_1(t)^\rho$ and $\alpha_2(t)^\rho$ are of the form $\alpha_1(t_1)\alpha_2(t_2)$.

(7.10) $\alpha_5(t)^\rho$ is of the form $\alpha_5(t_1)\alpha_{12}(t_2)$.

It can be verified easily by (2.1) that the center of the group generated by the elements $\alpha_1(t)$, $\alpha_2(t)$, $t \in K$, consists of the elements $\alpha_2(t)$, $t \in K$. From this, (7.7), and (7.8) that there exists a constant c_2 in K such that $\alpha_2(t)^\rho = \alpha_2(c_2 t)$ for all $t \in K$. Now take an element $h(\chi) \in \mathfrak{H}^1$ such that $\chi(\xi_3 + \xi_4) = c_2$, and define an inner automorphism ρ' of G^1 by $x^{\rho'} = h(\chi)^{-1}xh(\chi)$. Then $\alpha_2(t)^{\rho\rho'} = \alpha_2(t)$ for all $t \in K$, and all the statements (7.2)-(7.10) remain valid when ρ is replaced by $\rho\rho'$. Hence, for the proof of Theorem 7.1, we can furthermore assume

$$\alpha_2(t)^\rho = \alpha_2(t) \tag{7.11}$$

By (7.7) and (7.9) we can set

$$\alpha_1(t)^\rho = \alpha_1(c_1 t)\alpha_2(c' t^{2\theta+1}),$$

where c_1 and c' are constants in K. Combining this with the identity

$$\alpha_1(t)\alpha_1(u) = \alpha_1(t+u)\alpha_2(tu^{2\theta})$$

we obtain

$$c_1^{2\theta+1}tu^{2\theta} + c't^{2\theta+1} + c'u^{2\theta+1} = tu^{2\theta} + c'(t+u)^{2\theta+1}$$

for all $t, u \in K$. By setting $t = u = 1$ we have $c_1^{2\theta+1} = 1$, $c_1 = 1$. Then from the above it follows that $c'(t^{2\theta}u + tu^{2\theta}) = 0$ for all $t, u \in K$. From this and the assumption that K has more than 2 elements we can derive easily $c' = 0$. Thus $\alpha_1(t)^\rho = \alpha_1(t)$ for all $t \in K$. Similarly, we can prove $\alpha_5(t)^\rho = \alpha_5(t)$ for all $t \in K$. Thus

$$\alpha_1(t)^\rho = \alpha_1(t), \qquad \alpha_5(t)^\rho = \alpha_5(t). \tag{7.12}$$

Now, applying ρ to the identity (4.7) and using (7.8), (7.11), and (7.12), we obtain $c_3 = c_6 = c_7 = c_8 = c_9 = c_{10} = 1$. Similarly from (4.4) we obtain $c_4 = 1$. Thus we have proved $c_i = 1$ for all i. Thus

$$\alpha_i(t)^\rho = \alpha_i(t) \qquad (i = 1, 2, \cdots, 12) \tag{7.13}$$

By setting $r = \xi_2$, ξ_4 in (3.10) we obtain, respectively,

$$\alpha'_{12}(t) = \alpha_5(t^{1-2\theta})^{-1} h' \omega' \alpha_5(t^{1-2\theta}),$$
$$\alpha'_2(u) = \alpha_1(u^{1-2\theta})^{-1} h'' \omega'' \alpha_1(u^{1-2\theta}),$$

where: $\omega' = \omega(w(-1, 1, \infty))$; $\omega'' = \omega(w(1, -1, \infty))$; h' is an element in $\mathfrak{H}^1$ which commutes with ω'' and the elements $\alpha_1(t)$, $t \in K$; h'' is an element in $\mathfrak{H}^1$ which commutes with ω' and the elements $\alpha_5(t)$, $t \in K$. Since $w(-1, 1, \infty) w(1, -1, \infty) = w(-1, -1, \infty)$, we can assume $\omega' \omega'' = \omega_0 = \omega(w(-1, -1, \infty))$. Then, since $(\alpha_1(t), \alpha_5(u)) = 1$, we have from the above,

$$\alpha'_2(u) \alpha'_{12}(t) = (\alpha_1(u^{1-2\theta}) \alpha_5(t^{1-2\theta}))^{-1} h \omega_0 \alpha_1(u^{1-2\theta}) \alpha_5(t^{1-2\theta})$$

with $h = h'h'' \in \mathfrak{H}^1$. We have from (7.5)

$$\begin{aligned}(\alpha'_2(u) \alpha'_{12}(t))^\rho &= (\omega_0 \alpha_2(u) \alpha_{12}(t) \omega_0^{-1})^\rho \\ &= \alpha'_2(\chi_0(\xi_3 + \xi_4)^{-1} u) \alpha'_{12}(\chi_0(\xi_1 + \xi_2)^{-1} t) \\ &= a^{-1} h h(\chi_0) \omega_0 a \\ &= \alpha'_2(u) \alpha'_{12}(t) a^{-1} \omega_0^{-1} h(\chi_0) \omega_0 a\end{aligned}$$

where $a = \alpha_1(u^{1-2\theta}) \alpha_5(t^{1-2\theta})$. From this and the relations

$$\omega_0^{-1} h(\chi_0) \omega_0 = h(\chi_0)^{-1}, \qquad \mathfrak{U}^1 \mathfrak{H}^1 \cap \mathfrak{V}^1 = \{1\},$$

we can deduce easily $h(\chi_0) = 1$. Hence (7.5) yields

$$\omega_0^\rho = \omega_0 \tag{7.14}$$

Since the group G^1 is generated by ω_0 and $\alpha_1(t), \cdots, \alpha_{12}(t)$, $t \in K$, we can conclude from (7.13) and (7.14) that $\rho = 1$. Thus Theorem 7.1 is proved except for the uniqueness part.

The uniqueness part, however, can be proved just as the corresponding part of Theorem 9.1 of [4], if one uses the fact that ω_0 belongs to the group generated by the elements $\alpha_1(1)$, $\alpha_2(1)$, $\alpha_5(1)$, $\alpha_{12}(1)$, $\alpha'_1(1)$, $\alpha'_2(1)$, $\alpha'_5(1)$, $\alpha'_{12}(1)$. Thus the proof of Theorem 7.1 is complete.

UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, B. C.

REFERENCES.

[1] E. Cartan, "Oeuvres complètes," Part 1, vol. 1, *Gauthier-Villars*, Paris, 1952.

[2] C. Chevalley, "Sur certains groupes simples," *Tôhoku Mathematical Journal* (2), vol. 7 (1955), pp. 14-66.

[3] Séminaire C. Chevalley, "Classification des groupes de Lie algébriques," vol. 2, Paris, 1956-58.

[4] Rimak Ree, "A family of simple groups associated with the simple Lie algebra of type (G_2)," *American Journal of Mathematics*, vol. 83 (1961), pp. 432-462.

[5] Michio Suzuki, "A new type of simple groups of finite order," *Proceedings of the National Academy of Sciences*, vol. 46 (1960), pp. 868-870.

[6] E. Artin, "The orders of the classical simple groups," *Communications on Pure and Applied Mathematics*, vol. 8 (1955), pp. 455-472.

[7] R. Steinberg, "Variations on a theme of Chevalley," *Pacific Journal of Mathematics*, vol. 9 (1959), pp. 875-891.

[8] ———, "Automorphisms of finite linear groups," *Canadian Journal of Mathematics*, vol. 12 (1960), pp. 606-615.

[9] J. Tits, "Sur les analogues algébriques des groupes semi-simples complexes," *Colloque d'algèbre supérieure*, Bruxelles, 1956, pp. 261-289.

[10] ———, "Les groupes simples de Suzuki et de Ree," *Séminaire Bourbaki*, December, 1960.

THE STRUCTURE OF FROBENIUS ALGEBRAIC GROUPS.*

By David Hertzig.[1]

---

1. **Introduction.** A finite group G is called a Frobenius group if it has a proper subgroup H which is "disjoint" from all of its conjugates (i. e. $xHx^{-1} \cap H \neq \{e\}$ implies $x \in H$). The set $M = \{G - \bigcup_{x \in G} xHx^{-1}\} \cup \{e\}$ is then easily seen to be a normal subgroup, called the regular subgroup of G. The structure of M has been greatly studied and a long outstanding conjecture that M is necessarily nilpotent has recently been proved by J. Thompson [4].

In this paper we study the structure of Frobenius algebraic groups. An algebraic group G is called a *Frobenius algebraic group* if it has a proper algebraic subgroup H such that for all $x \in G$, $xHx^{-1} \cap H \neq \{e\}$ implies $x \in H$. Denote $M = \{G - \bigcup_{x \in G} xHx^{-1}\} \cup \{e\}$. This notation will be kept throughout the paper.

The simple counting techniques of the finite theory are no longer available and consequently the nature of the study of Frobenius algebraic groups is necessarily quite different from that of the finite theory. For example, the fact that M is a subgroup does not come out until quite late (Theorem 4). In the finite case this is proved by Frobenius using the theory of characters. For properties of finite Frobenius groups see [3].

The theory of algebraic groups is assumed. The reader is referred to [1] and [2] for the standard theorems and terminology. In particular, if G is an algebraic group, G_0 denotes the connected component of the identity element e; G_0 is a normal algebraic subgroup of finite index in G. A Borel subgroup of G is a maximal connected solvable algebraic subgroup. A torus of G is a connected diagonalizable subgroup. The set of semisimple (i. e. diagonalizable) elements of G is denoted G_s; the set of unipotent elements of G is denoted G_u. A unipotent group, i. e., one for which $G = G_u$, is nilpotent. If a Borel subgroup of G is nilpotent then G is nilpotent; in particular if a maximal torus of G is reduced to $\{e\}$ G is nilpotent. In general p will denote the characteristic of the ground field.

The author wishes to express his gratitude to Professor I. N. Herstein for suggesting these investigations as well as for many stimulating and helpful conversations.

---

* Received August 18, 1960.

[1] The work of the author was supported by OOR Project, Contract No. DA-30-115-ORD-976.

2. Basic properties of Frobenius groups. For $g \in G$ we define the rational map $\sigma_g\colon G \to G$ by $\sigma_g(x) = gxg^{-1}x^{-1}$. If N is a subgroup of G normalized by g then clearly $\sigma_g(N) \subset N$, and if N is a normal subgroup of G, σ_g induces a map (still denoted σ_g) $\sigma_g\colon G/N \to G/N$.

LEMMA 1. *Let G be a Frobenius algebraic group and $N \supset N_1$ algebraic subgroups of G with N_1 normal in N and such that H normalizes N and N_1. Then*

a) *for all $h \in H$, $h \neq e$, σ_h is injective on N if and only if $N \cap H = \{e\}$;*

b) *if σ_h is injective on N and surjective on N_1 then σ_h is injective on N/N_1;*

c) *if σ_h is surjective on N_1 and on N/N_1 then σ_h is surjective on N.*

Proof. a) Let $n \in N \cap H$; then $\sigma_n(n) = e = \sigma_n(e)$, hence $n = e$. Conversely $\sigma_h(n) = \sigma_h(n')$ implies $nhn^{-1} = n'hn'^{-1}$ and so $n^{-1}n'Hn'^{-1}n \cap H \neq \{e\}$. Therefore $n^{-1}n' \in H \cap N = \{e\}$ and $n = n'$.

b) Suppose $\sigma_h(n) = \sigma_h(n')n_1$ with $n, n' \in N$, $n_1 \in N_1$. Then $n'^{-1}n_1n' \in N_1$ and so $n'^{-1}n_1n' = \sigma_h(n'_1)$ for some $n'_1 \in N_1$. Therefore $\sigma_h(n) = \sigma_h(n')n_1 = \sigma_h(n')n'\sigma_h(n'_1)n'^{-1} = \sigma_h(n'n'_1)$. By hypothesis σ_h is injective on N, so $n = n'n'_1$ and σ_h is injective on N/N_1.

c) Let $n \in N$; then σ_h surjective on N/N_1 implies $n = \sigma_h(n')n_1$ with $n' \in N$, $n_1 \in N_1$. As in the proof of (b) there exists $n'_1 \in N_1$ such that $n = \sigma_h(n'n'_1)$. q. e. d.

LEMMA 2. *Let G be a Frobenius algebraic group and N a solvable algebraic subgroup of G normalized by H. For $h \in H$, if σ_h is injective on N then σ_h is surjective on N.*

Proof. First suppose N connected. If N is commutative σ_h is a homomorphism of N into N and since σ_h is injective $\sigma_h(N)$ and N have the same dimension, hence $\sigma_h(N) = N$. We proceed by induction on the dimension of N. Let N_1 be the commutator subgroup of N; since N is solvable N_1 is of strictly smaller dimension and by the induction hypothesis σ_h is surjective on N_1. By Lemma 1b σ_h is injective on N/N_1, which is commutative, hence σ_h is surjective on N/N_1. Therefore by Lemma 1c σ_h is surjective on N.

In the general case, by what we have already proved σ_h is surjective on N_0 so by Lemma 1b σ_h is injective on N/N_0, which is finite. Therefore σ_h is surjective on N/N_0 and applying Lemma 1c we have σ_h surjective on N.

q. e. d.

LEMMA 3. *Let G be a Frobenius algebraic group and N a solvable normal algebraic subgroup of G such that $N \cap H = \{e\}$. Let ρ be a rational representation of G with kernel N, $\bar{G} = \rho(G)$, $\bar{H} = \rho(H)$. Then $\bar{G}$ is a Frobenius algebraic group.*

Proof. Let $\bar{x} \in \bar{G}$ such that $\bar{x}\bar{H}\bar{x}^{-1} \cap \bar{H} \neq \{\bar{e}\}$. Then if $\bar{x} = \rho(x)$ there exist, $h, h_1 \in H$, $h \neq e$, $h_1 \neq e$, and $n \in N$ such that $xh_1x^{-1} = h^{-1}n$. By Lemma 1a σ_h is injective on N hence by Lemma 2 σ_h is surjective on N; let $n = \sigma_h(n_1)$. Then $xh_1x^{-1} = h^{-1}n = h^{-1}\sigma_h(n_1) = n_1h^{-1}n_1^{-1}$ and so $n_1^{-1}xHx^{-1}n_1 \cap H \neq \{e\}$; therefore $n_1^{-1}x \in H$ and $\bar{x} = \rho(n_1^{-1}x) \in \bar{H}$. q. e. d.

PROPOSITION 1. *Let G be a Frobenius algebraic group. Then $H \cap G_0 = H_0$ and if H is not finite, $H_0 = T$ is a maximal torus of G, G_0 is solvable, $M = G_{0u}$ and $G = H \cdot M$.*

Proof. Suppose H is finite and let $K = H \cap G_0$; if $s \in K_s$, $s \neq e$, then s belongs to a maximal torus T of G_0. If $x \in G_0$ centralizes T, $xsx^{-1} = s \in H \cap xHx^{-1}$ and $x \in K$ so that $T \subset K$ and $T = \{e\}$ which is impossible. Therefore $K = K_u$; let $u \in K$, $u \neq e$. Then $u \in B_u$ for some Borel subgroup B of G and since B_u is unipotent it is nilpotent and consequently has a positive dimensional center Z. If $x \in Z$, $xux^{-1} = u \in H \cap xHx^{-1}$, hence $x \in K$, therefore $Z \subset K$ which is a contradiction. Therefore $K = H \cap G_0 = \{e\} = H_0$.

We suppose then H is not finite, i.e., $H_0 \neq \{e\}$. If $x \in G$ normalizes H_0 then $x \in H$ and so H_0 is equal to its connected normalizer in G. If H_0 is unipotent it is nilpotent, hence is a Cartan subgroup of G_0 and $G_0 = H_0$ so that G normalizes H_0, hence $G = H$ contrary to assumption that H is a proper subgroup of G. Therefore a maximal torus S of H_0 is $\neq \{e\}$ and since S is contained in a maximal torus T of G_0 and T centralizes S, $T \subset H$ and $T = S$.

Let B_1 be a Borel subgroup of H_0 containing T and B a Borel subgroup of G_0 containing B_1. Then $B \cap H_0$ is a solvable subgroup of H_0 containing B_1, which is maximal solvable, hence $B_1 = B \cap H_0$. Similarly, since $(B \cap H)_0 \subset H_0, B_1 = B \cap H_0 = (B \cap H)_0$. Therefore $B_{1u} = B_u \cap H_0 = (B_u \cap H)_0$.

Let $x \in B_u$ normalize B_{1u}; then if $B_{1u} \neq \{e\}$, $xHx^{-1} \cap H \neq \{e\}$ and $x \in H$, so that B_{1u} is equal to its connected normalizer in B_u. Since B_u is a connected nilpotent group, it follows that $B_u = B_{1u}$ and since $B = T \cdot B_u$, $B = B_1 \subset H$. Let $g \in G_0$; then gBg^{-1} is a Borel subgroup of G_0 and since any two Borel subgroups contain a common maximal torus, $gHg^{-1} \cap H \neq \{e\}$ and $g \in H$, i.e. $G_0 \subset H$. Hence $G_0 = H_0$ and $G = H$ contrary to hypothesis.

Therefore $B_{1u} = \{e\}$ and $B_1 = T$ so that $H_0 = T$. Let $K = H \cap G_0$ and suppose $u \in K_u$, $u \neq e$. Then $u \in B_u$ for some Borel subgroup B of G_0 and since $B_u \neq \{e\}$ the connected center Z of $B_u \neq \{e\}$. Let $x \in Z$; since $xux^{-1} = u \in H \cap xHx^{-1}$, $x \in H$, i. e. $Z \subset H$, hence $Z \subset H_0 = T$ which is impossible since Z is unipotent. Therefore $K_u = \{e\}$ and $K = K_s$. Let $s \in K_s$, $s \neq e$; then s is in some maximal torus gTg^{-1} of G_0 and so $s \in H \cap gHg^{-1}$. Therefore $g \in H$ and $gTg^{-1} = T$, i. e. $s \in H_0$ and $K = H \cap G_0 = H_0$. Moreover $N_G(H_0) \subset H$ and so $N_{G_0}(H_0) \subset H \cap G_0 = H_0$, hence $N_{G_0}(T) = T$ and the Weyl group of G_0 is trivial, i. e. G_0 is solvable.

Let $x \in G$; xTx^{-1} is a maximal torus of G_0, hence $xTx^{-1} = yTy^{-1}$ with $y \in G_{0u}$ and $y^{-1}x \in H$ so that $G = G_{0u}H$. Since $G_{0u} \cap H \subset G_0 \cap H = H = T$, $G_{0u} \cap H = \{e\}$ and $G = G_{0u} \cdot H$.

By Lemma 1a, for all $h \in H$, $h \neq e$, σ_h is injective on G_{0u} and so by Lemma 2, σ_h is surjective on G_{0u}. Let $g \in M$, $g \neq e$, $g = hu$, $u \in G_{0u}$, $h \in H$. If $h \neq e$, $u = \sigma_{h^{-1}}(g_0)$ and $g = g_0 h g_0^{-1}$ which is impossible. Therefore $h = e$ and $M \subset G_{0u}$. Conversely, since $G_{0u} \cap H = \{e\}$, $G_{0u} \cap \bigcup_{x \in G} xHx^{-1} = \{e\}$ and $G_{0u} \subset M$, hence $G_{0u} = M$. q. e. d.

Proposition 1 gives the desired structure theorem for Frobenius algebraic groups in the case H not finite. For the remainder of this paper we adopt the convention: an algebraic group G is a *Frobenius algebraic group* if it has a proper finite algebraic subgroup H such that for all $x \in G$, $xHx^{-1} \cap H \neq \{e\}$ implies $x \in H$. Proposition 1 then asserts $H \cap G_0 = \{e\}$.

COROLLARY. *If G is a Frobenius algebraic group then $G_0 \subset M$.*

Proof. By Proposition 1 $G_0 \cap H = \{e\}$ and since G_0 is normal in G, $G_0 \cap \bigcup xHx^{-1} = \{e\}$. Therefore $G_0 \subset \{G - \bigcup_{x \in G} xHx^{-1}\} \cup \{e\} = M$. q. e. d.

3. A first structure theorem.

The corollary to Proposition 1 asserts $G_0 \subset M$ hence if M is a subgroup of G (as is proved later in Theorem 4) $G_0 = M_0$. Therefore a first approach to the study of the structure of M is through the structure of G_0. In this section we consider the special case where G_0 is assumed to be solvable.

THEOREM 1. *Let G be a Frobenius algebraic group and suppose G_0 is solvable. Then G_0 is nilpotent. Moreover, if $\dim G > 0$ either G_0 is a torus of dimension $d \equiv 0 \pmod{p-1}$, in which case H is a p-group, or G_0 is unipotent, in which case the order of H is prime to p.*

Proof. Let l be a prime dividing the order of H and let h be an element of H of order l. If $\dim G_u > 0$ G_u contains a characteristic subgroup A isomorphic to G_a (the one-dimensional additive group). Since $hAh^{-1} = A$

and no element of A centralizes h the map $\operatorname{ad} h\colon A \to A$ defined by $\operatorname{ad} h(a) = hah^{-1}$ induces a fixed-point-free automorphism Φ of G_a. Any automorphism of G_a is of the form $x \to \lambda x^{p^\nu}$ and since $\Phi^l = 1$ we must have $\Phi(x) = \lambda x$ where $\lambda^l = 1$ and $\lambda \neq 1$, hence $l \neq p$. Therefore if $\dim G_u > 0$ the order of H is prime to p.

Now let T_0 be a maximal torus of G_0; then hT_0h^{-1} is also a maximal torus of G_0, hence by conjugacy of maximal tori $hT_0h^{-1} = xT_0x^{-1}$ for some $x \in G_0$. By Proposition 1 and Lemma 1a, σ_h is injective on G_0 and by Lemma 2, σ_h is surjective on G_0 so we have $x = \sigma_h(g)$, $g \in G_0$. Therefore $hT_0h^{-1} = \sigma_h(g)T_0\sigma_h(g)^{-1} = hgh^{-1}g^{-1}T_0ghg^{-1}h^{-1}$, i.e. if $T = g^{-1}T_0g$, $hTh^{-1} = T$. If $d = \dim T$ and n is an integer prime to p the subgroup T_n of elements of T of order n contains exactly n^d elements. Clearly $hT_nh^{-1} = T_n$ and no element of T centralizes H. It follows that $n^d \equiv 1 \pmod{l}$. Therefore if $l \neq p$, in particular $l^d \equiv 1 \pmod{l}$ and so $d = 0$, $T = \{e\}$ and G_0 is unipotent. If H is a p-group, G_0 is a torus and $n^d \equiv 1 \pmod{p}$ for all n prime to p implies $d \equiv 0 \pmod{p-1}$. q. e. d.

4. Fixed-point free automorphisms. An automorphism Φ of a group G is said to be fixed-point-free if the only element of G left fixed by Φ is the identity element. If G is a Frobenius algebraic group and $h \in H$, $h \neq e$, then (assuming M to be a subgroup) $\operatorname{ad} h\colon x \to hxh^{-1}$ induces a fixed-point-free automorphism of M. Conversely, if an algebraic group M admits a rational fixed-point-free automorphism Φ of prime order then, if H denotes the group generated by Φ, the split extension of H by M is a Frobenius algebraic group. The following statements are translations of the corresponding results on Frobenius groups into the language of automorphisms. The proofs of Lemmas 1′, 2′ and 3′ are identical to the proofs of the corresponding results on Frobenius groups; it is clear that here we need no restriction on the order of Φ. If Φ is an automorphism of G, we denote $\bar{\Phi}$ the map of G into G defined by $\bar{\Phi}(x) = \Phi(x)x^{-1}$.

LEMMA 1′. *Let G be an algebraic group, Φ a rational automorphism of G and $N \supset N_1$ algebraic subgroups of G, stable under Φ, with N_1 normal in N. Then*

a) *$\bar{\Phi}$ is injective on N if and only if Φ is fixed-point-free on N;*

b) *if $\bar{\Phi}$ is injective on N and surjective on N_1 then $\bar{\Phi}$ is injective on N/N_1, i.e. if Φ acts fixed-point freely on N and $\bar{\Phi}$ is surjective on N_1 then Φ induces a fixed-point-free automorphism of N/N_1;*

c) *if $\bar{\Phi}$ is surjective on N_1 and on N/N_1 then $\bar{\Phi}$ is surjective on N.*

Lemma 2′. *Let Φ be an automorphism of the algebraic group G and N a solvable algebraic subgroup of G stable under Φ and such that Φ acts fixed-point freely on N. Then $\bar{\Phi}$ is surjective on N.*

Lemma 3′. *Let G be an algebraic group admitting a fixed-point-free rational automorphism Φ and N a solvable normal algebraic subgroup of G stable under Φ. Then Φ induces a fixed-point-free automorphism of G/N.*

Lemma 4. *Let G be a connected algebraic group admitting a fixed-point-free rational automorphism of finite period n. Then for all $x \in G$,*

$$\Phi^{n-1}(x)\Phi^{n-2}(x)\cdots\Phi(x)x = e.$$

Proof. For $x, y \in G$ we define $y \circ x = \Phi(y)xy^{-1}$. Then $e \circ x = x$ and $z \circ (y \circ x) = (zy) \circ x$ so that G acts on itself as a transformation space. The isotropy subgroup of e consists precisely of the fixed-points of Φ, hence is reduced to $\{e\}$. Therefore the orbit U of e is an open subset of G (in fact, U is a principal homogeneous space for G). If $g \in U$ we may write $g = \Phi(y)y^{-1}$, hence $\Phi^{n-1}(g)\Phi^{n-2}(g)\cdots\Phi(g)g = e$ for all $g \in U$. Since U is dense in G the assertion of the lemma follows immediately. q. e. d.

Lemma 5. *Let Φ be a fixed-point-free rational automorphism of a torus T. Then if the order of Φ is finite, it is a power of p and if s is prime to p, Φ^s is also fixed-point-free.*

Proof. Suppose $\Phi^n = 1$ and let l be a prime different from p dividing n, say $n = lm$. Let $F = \{x \in T, \Phi^l(x) = x\}$; then F_0 is a torus admitting a fixed-point-free automorphism of period $l \neq p$ and so by Theorem 1 F is finite of order $\equiv 1 \pmod{l}$. Let $T_1 = T/F$ and $F_1 = \{\bar{x} \in T_1, \Phi^m(\bar{x}) = \bar{x}\}$. If $\bar{x} \in T_1$ is such that $\bar{x}^{-1}\Phi^m(\bar{x}) \in F_1$ then $\bar{x}^{-1}\Phi^m(\bar{x}) = \Phi^m(\bar{x})^{-1}\Phi^{2m}(\bar{x}) = \cdots = \Phi^{(l-1)m}(\bar{x})^{-1}\Phi^{lm}(\bar{x})$ and so $[\bar{x}^{-1}\Phi^m(\bar{x})]^l = \bar{e}$, i. e. $[x^{-1}\Phi^m(x)]^l \in F$ and since the order of F is $\equiv 1 \pmod{l}$, $x^{-1}\Phi^m(x) \in F$, hence $\bar{x} \in F_1$. Therefore Φ^m acts fixed-point freely on the torus T_1/F_1 so by Theorem 1 $T_1 = F_1$, i. e. $\Phi^m = 1$ on T_1. Therefore the homomorphism $\rho\colon x \rightarrow x^{-1}\Phi^m(x)$ maps T into F and the image of ρ has dimension 0. Therefore $T =$ kernel of ρ, that is to say $\Phi^m = 1$ on T. Proceeding in this manner we finally have $\Phi^{p^r} = 1$ on T for some power r of p.

If $(s, p) = 1$ then $as + bp^r = 1$ and $\Phi = \Phi^{as}$. Therefore if $x = \Phi^s(x)$, we have $x = \Phi^{as}(x) = \Phi(x)$ so $x = e$. q. e. d.

Lemma 6. *Let Φ be a fixed-point-free rational automorphism of a unipotent group G. Then Φ^{p^r} also is fixed-point-free.*

Proof. Let $F = \{x \in G, \Phi^{p^r}(x) = x\}$. Since G is unipotent, hence nilpotent, so is the subgroup F and if $F \neq \{e\}$ then there exists an element $x \neq e$ in the center of F. The group H generated by $x, \Phi(x), \cdots, \Phi^{p^r-1}(x)$ is a finitely generated commutative group, hence a finite p-group. But H admits the fixed-point-free automorphism Φ of period a power of p, hence must have order $\equiv 1 \pmod{p}$, which is impossible. Therefore $F = \{e\}$ and Φ^{p^r} is fixed-point-free. q. e. d.

THEOREM 1′. *Let G be a connected solvable algebraic group admitting a fixed-point-free rational automorphism Φ of order n. Then if n is prime to p, G is unipotent and if n is a power of p, G is a torus. In particular, if n is a power of a prime G is nilpotent. Also, if the restriction of Φ to G_u has order prime to p, G is nilpotent.*

Proof. Let T_1 be a maximal torus of G; then $\Phi(T_1) = xT_1x^{-1}$ and writing $x = \Phi(y)y^{-1}$ (Lemma 2′) the torus $T = y^{-1}T_1y$ is stable under Φ. Since $G = T \cdot G_u$ the first assertion of the theorem is an immediate consequence of Lemmas 5 and 6.

Now suppose the restriction of Φ to G_u has order s prime to p. For $t \in T$, $u \in G_u$, $\Phi^s(tut^{-1}) = \Phi^s(t)\Phi^s(u)\Phi^s(t)^{-1}$ and so $tut^{-1} = \Phi^s(t)u\Phi^s(t)^{-1}$, i. e. $t^{-1}\Phi^s(t)$ centralizes G_u for all $t \in T$. By Lemma 5, Φ^s is fixed-point-free on T and by Lemma 2′ every element of T is of the form $t^{-1}\Phi^s(t)$. Therefore T is in the center of G and $G = T \times G_u$ is nilpotent. q. e. d.

We have seen in the proof of Theorem 1′ that there is a maximal torus T of G stable under Φ and by Lemma 5 the restriction of Φ to T has order a power of p. If m is any integer prime to p the subgroup T_m of elements of T of order m has order m^d where $d = \dim T = $ rank of G. Since T_m admits Φ fixed-point freely $m^d \equiv 1 \pmod{p}$. Therefore we must have $d \equiv 0$ (mid $p-1$).

COROLLARY. *If the algebraic group G admits a fixed-point-free rational automorphism of finite order then G is solvable of rank $d \equiv 0 \pmod{p-1}$.*

PROPOSITION 2. *Let G be an algebraic group admitting a fixed-point-free rational automorphism Φ of period 2. Then G is commutative and Φ is inversion. Moreover, if $p = 2$, G_0 is a torus and if $p \neq 2$, G_0 is unipotent.*

Proof. By Lemma 4 for all $x \in G_0$, $\Phi(x)x = e$, hence $\Phi(x) = x^{-1}$ and G_0 is commutative. Applying Lemmas 2′ and 1′ we have Φ is injective on G/G_0, hence surjective on G/G_0 since G/G_0 is finite. Then by Lemma 1′c, $\bar{\Phi}$ is surjective on G and therefore for all $x \in G$, $\Phi(x)x = e$, i. e. Φ is inversion and G is commutative.

Since Φ acts fixed-point freely, G has no elements of order 2 and so if $p = 2$, G_0 is a torus and if $p \neq 2$, G_0 is unipotent. q. e. d.

LEMMA 7. *Let G be a connected algebraic group admitting a fixed-point-free rational automorphism Φ of period 3. Then G is nilpotent.*

Proof. By Lemma 4 for all $x \in G$, $\Phi^2(x)\Phi(x)x = e$ and hence also $\Phi^2(x^{-1})\Phi(x^{-1})x^{-1} = e$, i.e. $x\Phi(x)\Phi^2(x) = e$. Therefore $\Phi^2(x^{-1}) = x\Phi(x) = \Phi(x)x$, i.e. for all $x \in G$, x commutes with $\Phi(x)$. Let K be the subgroup of G generated by x and $\Phi(x)$; K is a commutative group stable under Φ and so by Lemma 2′, $\bar{\Phi}$ is surjective on K. Hence $\bar{\Phi}$ is surjective on G.

Let B_0 be a Borel subgroup of G; then $\Phi(B_0)$ is also a Borel subgroup, hence by conjugacy $\Phi(B_0) = xBx^{-1}$. Since $\bar{\Phi}$ is surjective, $x = \bar{\Phi}(y)$ for some $y \in G$. Then it follows that $B = y^{-1}B_0y$ is a Borel subgroup of G stable under Φ. By Theorem 1′, B is nilpotent and hence $G = B$ is nilpotent.

q. e. d.

THEOREM 2. *Let G be a semi-simple algebraic group and Φ a rational automorphism of G. Then Φ has a non-trivial fixed-point.*

Proof. We assume Φ acts fixed-point freely on G and arrive at a contradiction. The automorphisms of the semi-simple algebraic groups are known to be of the form $\Phi(x) = ax^\sigma a^{-1}$ where σ is an "outer" automorphism and is of finite order, $\sigma^r = 1$. When G is simple and $r > 1$ we may have either $r = 2$ (type A_n, D_n, E_6) or $r = 3$ (type D_4). By repeated application of Φ we have $\Phi^r(x) = bxb^{-1}$ where $b = \Phi^{r-1}(a) \cdots \Phi(a)a = aa^\sigma \cdots a^{\sigma^{r-1}}$, hence $b^\sigma = a^{-1}ba$. Then $\Phi(b) = ab^\sigma a^{-1} = b$ and so $b = e$ and $\Phi^r = 1$.

Let G' be one of the simple components of G; since the simple components of G are uniquely determined, $\Phi^i(G')$ is a simple component of G for each i, $0 \leqq i < r$. They cannot all be distinct for otherwise if $x \in G'$ the representation $\Phi^{r-1}(x) \cdots \Phi(x)x = e$ given by Lemma 4 would imply $x = e$. Therefore for some i, $0 < i < r$, $\Phi^i(G') = G'$. Let $d = (i, r)$ and $ai + br = d$; then $\Phi^d = \Phi^{ai}$, hence $\Phi^d(G') = G'$. Choose $d \mid r$ such that $\Phi^d(G') = G'$ and $G', \Phi(G'), \cdots, \Phi^{d-1}(G')$ are all distinct. Let $x \in G'$ be such that $\Phi^d(x) = x$; then if $y = \Phi^{d-1}(x) \cdots \Phi(x)x$, $\Phi(y) = y$ and so $y = e$ which implies $x = e$. Therefore Φ^d is a fixed-point-free automorphism of G' of order r/d. Replacing G by G' and Φ by Φ^d we have reduced our considerations to the case of a simple group G. But in this case $r = 2$ or 3 and then Proposition 2 and Lemma 7 imply G must be nilpotent, which is impossible since G is simple.

q. e. d.

THEOREM 3′. *Let G be a connected algebraic group admitting a fixed-point-free rational automorphism Φ. Then G is solvable. Moreover, if Φ is of finite order n prime to p, G is unipotent and if Φ is of order a power of p, G is a torus.*

Proof. Let R be the radical of G; R is a connected solvable characteristic algebraic subgroup of G. By Lemma 3′ the semi-simple algebraic group G/R admits a fixed-point-free automorphism so by Theorem 2, $G = R$ is solvable. The remaining assertion of the theorem now follows immediately from Theorem 1′. q. e. d.

5. A second structure theorem. Our first structure theorem (Theorem 1) asserts that if G is a Frobenius algebraic group such that G_0 is solvable then G_0 is nilpotent. The results of the preceding section allow us to remove the assumption of solvability.

THEOREM 3. *Let G be a Frobenius algebraic group. Then G_0 is nilpotent. Moreover, either G_0 is a torus of dimension $d \equiv 0 \pmod{p-1}$ and H is a p-group, or G_0 is unipotent and the order of H is prime to p.*

Proof. Let l be a prime dividing the order of H and let h be an element of H of order l. Since $hG_0h^{-1} = G_0$ and no element of G_0 centralizes h the map $\operatorname{ad} h\colon G_0 \to G_0$ defined by $\operatorname{ad} h(g) = hgh^{-1}$ is a fixed-point-free automorphism of G_0 of period l. By Theorem 3′, G_0 is nilpotent and the assertion of the theorem is an immediate consequence of Theorem 1. q. e. d.

6. The regular subgroup of a Frobenius algebraic group. Recall that if G is a Frobenius group we denote $M = \{G - \bigcup_{x \in G} xHx^{-1}\} \cup \{e\}$ and a theorem of Frobenius asserts M is a normal subgroup of G in the case G finite. We are now in a position to extend this theorem to algebraic groups.

THEOREM 4. *If G is a Frobenius algebraic group then M is a normal algebraic subgroup, called the regular subgroup of G.*

Proof. Let ρ be a rational representation of G with kernel G_0, $\bar{G} = \rho(G)$, $\bar{H} = \rho(H)$. Since G_0 is nilpotent (Theorem 3) Proposition 1 and Lemma 3 imply $\bar{G}$ is a Frobenius algebraic group. Since $\bar{G}$ is finite, $\bar{M}$ is a normal subgroup of $\bar{G}$. Let $g \in G$, $g \notin M$; then there exists $h \in H$, $h \neq e$, and $x \in G$ *such that* $g = xhx^{-1}$ and so $\bar{g} = \rho(g) \in \bigcup_{\bar{x} \in \bar{G}} \bar{x}\bar{H}\bar{x}^{-1}$. Moreover, since $G_0 \cap H = \{e\}$, $G_0 \cap \bigcup_{x \in G} xHx^{-1} = \{e\}$, hence $g \notin G_0$, i. e. $\bar{g} \neq \bar{e}$. Therefore $\bar{g} \notin \bar{M}$ and $M \supset \rho^{-1}(\bar{M})$.

Suppose now $g \in M$; if $g \in G_0$ then $\bar{g} = \rho(g) = \bar{e} \in \bar{M}$. If $g \notin G_0$ and if $\bar{g} \in \bigcup_{\bar{x} \in \bar{G}} \bar{x}\bar{H}\bar{x}^{-1}$ there exists $x \in G$ and $h \in H$, $h \neq e$, such that $hx^{-1}gx \in G_0$. By Lemmas 1a and 2, σ_h is surjective on G_0 and there exists $g_0 \in G_0$ such that $hx^{-1}gx = \sigma_h(g_0) = hg_0h^{-1}g_0^{-1}$, i. e. $g = xg_0h^{-1}g_0x^{-1} \in \bigcup_{x \in G} xHx^{-1}$ which is impossible since $g \in M$. Therefore $\bar{g} \notin \bigcup_{\bar{x} \in \bar{G}} \bar{x}\bar{H}\bar{x}^{-1}$, i.e. $\bar{g} \in \bar{M}$ and $M \subset \rho^{-1}(\bar{M})$. Consequently $M = \rho^{-1}(\bar{M})$ and therefore M is a normal subgroup of G.

q. e. d.

THEOREM 5. *Let G be a Frobenius algebraic group and M the regular subgroup of G. Then $G = H \cdot M$, M_0 is nilpotent and either $M = M_s$ and H is a p-group or M_0 is unipotent and the order of H is prime to p. In any case, M_0 and M/M_0 are nilpotent and so M is solvable.*

Proof. By Theorem 3, G_0 is nilpotent and so by Lemma 3, if ρ is a rational representation of G with kernel G_0 then $\rho(G)$ is a finite Frobenius group (with regular subgroup $\rho(M)$). In the finite case then we have easily $\rho(G) = \rho(H) \cdot \rho(M)$. By the corollary to Proposition 1, $G_0 \subset M$ and it follows that $G = HM$; since $H \cap M = \{e\}$, $G = H \cdot M$. Also since $G_0 \subset M$, $M_0 = G_0$ and the next assertion follows from Theorem 3. By Thompson's theorem [4] M/M_0 is nilpotent.

q. e. d.

7. An application. As a consequence of his theorem Thompson was able to prove a theorem concerned with maximal subgroups of a finite group [4]. The following is an extension to algebraic groups.

THEOREM 6. *Let G be an algebraic group and suppose that one of the maximal subgroups M of G is nilpotent. Then G_0 is solvable. If $[M : M_0]$ is odd, then G is solvable.*

Proof. If M is nilpotent so is $\bar{M}$ (smallest algebraic group containing M) and since M is maximal either $M = \bar{M}$ or $\bar{M} = G$; therefore we may assume M to be an algebraic subgroup of G. Since $M \subset N_G(M_0)$ (normalizer in G of M_0) either M_0 is normal in G or $M = N_G(M_0)$. Suppose first $M = N_G(M_0)$; then $M \supset N_{G_0}(M_0) = M \cap G_0 \supset M_0$, hence M_0 is a nilpotent subgroup of G_0 equal to its connected normalizer in G_0. Therefore M_0 is a Cartan subgroup of G_0 and is maximal nilpotent; since $M \cap G_0$ is nilpotent either $M \cap G_0 = G_0$, in which case G_0 is nilpotent, or else, as we now assume, $M_0 = M \cap G_0 = C_{G_0}(T)$ (centralizer in G_0 of T) where T is a maximal torus of G_0. Note $M \subset N_G(T)$ and if $N_G(T) = G$, $N_{G_0}(T) = N_G(T) \cap G_0 = G_0$ hence T is normal in G_0 and G_0 is nilpotent; we assume then $M = N_G(T)$, hence $M_0 = M \cap G_0 = N_{G_0}(T) = C_{G_0}(T)$ so the Weyl group of G_0 is reduced to $\{e\}$, hence G_0 is solvable.

Now suppose M_0 normal in G; by considering a rational representation of G with kernel M_0 we are reduced to the case M finite. We proceed by induction on the order m of M, the case $m = 1$ being trivial. In particular, the induction hypothesis allows us to assume if $N \neq \{e\}$ is a normal subgroup of M then $N_G(N)=M$. Since $M\cap G_0=N$ is normal in M, if $N\neq\{e\}$ we have $N_G(N)=M$ and $N_{G_0}(N)=M\cap G_0=N$. Since N is nilpotent its center $Z(N)\neq\{e\}$; if $x\in Z(N)$, $x\neq e$, $C_G(x)\subset M$ hence $C_{G_0}(x)=N$. If $s\neq e$ is a semisimple element of $Z(N)$ then $s\in T$, T a maxmal torus of G_0 and $T\subset C_{G_0}(s)=N$ which is finite; therefore $T=\{e\}$ and G_0 is nilpotent. If $u\neq e$ is a unipotent element of $Z(N)$ then $u\in B_u$, B a Borel subgroup of G_0 and $Z(B_u)\subset C_{G_0}(u)=N$; therefore $B_u=\{e\}$ (since it is a connected nilpotent group and if $\dim B_u>0$, $\dim Z(B_u)>0$) and B, hence G_0, is a torus.

Finally then we may assume $M\cap G_0=N=\{e\}$. Let $H=Z(M)$; since M is nilpotent $H\neq\{e\}$. Let $G'=G_0H$ and suppose $x\in G'$ such that $xHx^{-1}\cap H\neq\{e\}$; say $x=gh$, $g\in G_0$, $h\in H$ and there exists $h'\in H$, $h'\neq e$, such that $gh'g^{-1}\in H$. Then $h'^{-1}gh'g^{-1}\in G_0\cap H=\{e\}$, hence $h'^{-1}gh'g^{-1}=e$, i.e. $gh'g^{-1}=h'$ and $g\in C_G(h')\subset M$. But $g\in G_0$ and $G_0\cap M=\{e\}$, so that $g=e$ and $x=h\in H$. Therefore G' is a Frobenius group and by Theorem 3, $G'_0=G_0$ is nilpotent.

Now let ρ be a rational representation of G with kernel G_0, $\rho(G)=\bar{G}$, $\rho(M)=\bar{M}$. Then $\bar{G}$ is a finite group, $\bar{M}$ a maximal subgroup of $\bar{G}$ which is nilpotent, and the order of $\bar{M}$ divides $[M:M_0]$. Therefore if $[M:M_0]$ is odd so is the order of $\bar{M}$ and it follows from [4] that $\bar{G}$ is solvable. Then G, being an extension of a solvable group by a solvable group, is solvable.

q. e. d.

Actually the structure of $\bar{G}=G/G_0$ can be completely determined also in the case $[M:M_0]$ even because Thompson has determined the structure of all finite groups having a maximal subgroup which is nilpotent [5].

CORNELL UNIVERSITY.

REFERENCES.

[1] A. Borel, "Groupes linéaires algébriques," *Annals of Mathematics*, vol. 64 (1956), pp. 20-82.

[2] C. Chevalley, "Classification des groupes de Lie algébriques," *Séminaire C. Chevalley* (1956-58), Ecole Normale Supérieure, Paris.

[3] W. Feit, "On the structure of Frobenius groups," *Canadian Journal of Mathematics*, vol. 9 (1957), pp. 587-596.

[4] J. Thompson, "Finite groups with fixed-point-free automorphisms of prime order," *Proceedings of the National Academy of Sciences*, vol. 45 (1959), pp. 578-581.

[5] ———, "A special class of non-solvable groups," *Mathematische Zeitschrift*, vol. 72 (1960), pp. 458-462.

A FAMILY OF SIMPLE GROUPS ASSOCIATED WITH THE SIMPLE LIE ALGEBRA OF TYPE (G_2).*

By Rimhak Ree.[1]

Introduction. In this paper we construct a family of simple groups. The family contains finite as well as infinite groups. The order of the finite groups in the family are

$$q^3(q-1)(q^3+1), \qquad \text{where } q = 3^{2n+1}, \qquad n = 1, 2, 3, \cdots.$$

By using the fact that the above orders are divisible by 8 but not by 16, one can show easily that none of the simple groups listed in [1] or [4] has any of the above orders.[2]

The construction is carried out by applying to the Chevalley groups of type (G_2) a method which emerges naturally when one interprets Suzuki's [5] construction of his simple groups from a Lie theoretical point of view. The Lie theoretical interpretation of Suzuki groups is as follows. Let $\mathfrak{g}$ be the simple Lie algebra of type (B_2) over the complex number field, and $\Sigma = \{\pm a, \pm b, \pm(a+b), \pm(2a+b)\}$ the set of roots of $\mathfrak{g}$. For an arbitrary field K, define the algebra $\mathfrak{g}_K$ over K and the automorphisms $x_r(t)$, where $r \in \Sigma$, $t \in K$, of $\mathfrak{g}_K$ as in [2], and let G be the group generated by all the $x_r(t)$. Now assume that K is a field of characteristic 2 which admits an automorphism $t \to t^\theta$ such that $2\theta^2 = 1$. By using a representation of G (given, for example, in [3]) one can show easily that the matrix $S(t, u)$ given by Suzuki in [5] corresponds to $\alpha(t)\beta(u)$, where

$$\alpha(t) = x_a(t^\theta) x_b(t) x_{a+b}(t^{2\theta+1}); \qquad \beta(t) = x_{a+b}(t) x_{2a+b}(t^{2\theta}).$$

The above expressions lead one to look for an automorphism σ of G such that the elements $\alpha(t)\beta(u)$ are exactly those elements in $\mathfrak{U}$ (the subgroup of G generated by all $x_r(t)$ with $r > 0$) which are left invariant by σ. It turns out that there exists indeed such an automorphism of G. It is given by

$$x_{\pm a}(t) \leftrightarrow x_{\pm b}(t^\theta), \qquad x_{\pm(a+2b)}(t) \leftrightarrow x_{\pm(a+b)}(t^\theta).$$

---

* Received September 19, 1960; revised February 21, 1961.

[1] This work was done while the author held a Research Associateship, 1959-1960, of the Office of Naval Research, U. S. Navy.

The author wishes to express gratitude to J. Tits for his persual of the manuscript and many valuable suggestions.

[2] See Theorems 8. 3 and 8. 5.

Denoting by $\mathfrak{B}$ the group generated by all $x_r(t)$ with $r < 0$, let $\mathfrak{U}^1$ (resp. $\mathfrak{B}^1$) be the group of elements in $\mathfrak{U}$ (resp. $\mathfrak{B}$) left invariant by σ. Then the group G^1 generated by $\mathfrak{U}^1$ and $\mathfrak{B}^1$ is simple when K has more thai 2 elements, and yields Suzuki groups when K is finite.

The Chevalley group G of type (G_2) happens to have a similar automorphism when K is a field of characteristic 3 which admits an automorphism $t \rightarrow t^\theta$ such that $3\theta^2 = 1$. Hence we can define the group G^1 in exactly the same way as above. As one of the main purposes of this paper we shall show that the group G^1 is simple when K has more that 3 elements.

In the case of Suzuki groups, G^1 turns out to be the group of *all* elements in G fixed by σ. For the groups of type (G_2) the same holds true when the field K is finite, but it is unknown whether or not one can, in general, dispense with the finiteness condition. Some efforts in this direction may be found in Section 8.

In the last section, we show that any automorphism of the *finite* simple group G^1 of type (G_2) can be written as the product of an inner automorphism and an automorphism induced by an automorphism of the ground field. The author has been unable to extend this result to the case of infinite groups.[3]

1. **Chevalley groups.** Although we shall use later only Chevalley groups of type (G_2), we treat here the Chevalley groups in general, since it does not make the exposition more complicated.

Let Σ be a simple root system. We fix an order in Σ so that we can talk about positive, negative, and fundamental roots. Let P (denoted in [2] by P_r) be the additive group generated by Σ. For r, s in Σ define the integer $s(r)$ by $s(r) = p - q$, where q (resp. $-p$) is the maximum (resp. minimum) integer i such that $s + ir$ is a root. Then for each $r \in \Sigma$, the map $s \rightarrow s(r)$ can be extended to a linear map on P. The symmetry w_r with respect to $r \in \Sigma$ is the permutation of Σ defined by $w_r(s) = s - s(r)r$. The Weyl group W of Σ is the group generated by all the w_r, $r \in \Sigma$.

Now we fix an arbitrary field K, and denote by K^* the multiplicative group of K. For $r \in \Sigma$ and $z \in K^*$, define the homomorphism $\chi_{r,z}\colon P \rightarrow K^*$ by $\chi_{r,z}(u) = z^{u(r)}$. Denote by X the group generated by all the $\chi_{r,z}$, where $r \in \Sigma$, $z \in K^*$. It can be shown that $w(s)(w(r)) = s(r)$ for any $r, s \in \Sigma$ and $w \in W$. From this it follows that $\chi \circ w \in X$ for any $\chi \in X$ and $w \in W$. It is shown in [2] that, for any pair of Σ and K, there exists a group G (denoted by G' in [2]), which we shall call the *Chevalley group* of type Σ over K, and elements $x_r(t)$, where $r \in \Sigma$, $t \in K$, in G such that the conditions (1.1)-(1.8), below, are satisfied:

---

[3] J. Tits remarks that the finiteness condition seems to be dispensed with if one uses his geometric interpretation of the group G^1 given in [7].

(1.1) G is generated by the elements $x_r(t)$, where $r \in \Sigma$, $t \in K$.

(1.2) For any two positive roots r and s in Σ,

we have

$$x_r(t)x_s(u)x_r(-t) = x_s(u) \prod_{i,j} x_{ir+js}(C_{ij;r,s}t^iu^j),$$

where the product is taken over all pairs (i, j) of integers such that $ir + js$ is a root, the pairs being arranged such that the roots $ir + js$ form an increasing sequence, and where $C_{ij;r,s}$ are certain integral constants depending only on Σ (not on K).

(1.3) For each $r \in \Sigma$, there exists a homomorphism ϕ: $SL(2; K\text{Q} \rightarrow G$ such that

$$\phi_r \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = x_{-r}(t), \qquad \phi_r \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = x_r(t), \qquad (t \in K).$$

(1.4) There exists a homomorphism $h: X \rightarrow G$ such that

$$h(\chi_{r,z}) = \phi_r \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}$$

for all $r \in \Sigma$ and $z \in K^*$.

(1.5) For any $\chi \in X$ and $r \in \Sigma$, we have

$$h(\chi)x_r(t)h(\chi)^{-1} = x_r(\chi(r)t), \qquad (t \in K).$$

(1.6) For

$$\omega_r = \phi_r \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

we have

$$\omega_r x_s(t)\omega_r^{-1} = x_{w_r(s)}(\eta_{r,s}t), \qquad (s \in \Sigma, t \in K),$$

where $\eta_{r,s}$ are certain integral constants ± 1 depending only on Σ (not on K).

(1.7) For any $r_1, \cdots, r_m \in \Sigma$ and any $\chi \in X$, we have

$$\omega h(\chi)\omega^{-1} = h(\chi')$$

where

$$\omega = \omega_{r_1} \cdots \omega_{r_m}$$

and where $\chi' \in X$ is defined by $\chi'(s) = \chi(w^{-1}(s))$ with

$$w = w_{r_1} \cdots w_{r_m}.$$

(1.8) If $r_1, \cdots, r_m \in \Sigma$ and $\chi \in X$ satisfy $\eta_s = \chi(s)$ for all $s \in \Sigma$, and if

$$w_{r_1} \cdots w_{r_m} = 1,$$

then

$$\omega_{r_1} \cdots \omega_{r_m} = h(\chi).$$

Here η_s are integers ± 1 defined from $r_1, \cdots, r_m$ by

$$\eta_s = \eta_{r_1, v_1(s)} \cdots \eta_{r_m, v_m(s)},$$

where

$$v_m = 1, v_{m-1} = w_{r_m}, v_{m-2} = w_{r_{m-1}} w_{r_m}, \cdots,$$
$$v_1 = w_{r_2} w_{r_3} \cdots w_{r_m}.$$

Note that the above properties (1.2)-(1.8) are all expressed in the form of "relations" of the generators $x_r(t)$. Therefore, by using the constants $C_{ij;r,s}$ and $\eta_{r,s}$ which arise from a Chevalley group, we can consider a group G abstractly defined by the generators and the relations (1.2)-(1.8). In order to distinguish this group G from the underlying Chevalley group which gives rise to the constants $C_{ij;r,s}$ and $\eta_{r,s}$, we shall denote the latter by $\hat{G}$, and let $x \to \hat{x}$ be the natural homomorphism of G onto $\hat{G}$. We shall show, in the rest of this section, that $x \to \hat{x}$ is an isomorphism. First we shall derive some consequences of (1.1)-(1.8).

(1.9) If $r = -a$, where a is a fundamental root, and if s is a positive root, then we have an identity of the form given in (1.2).

Proof. Since a is fundamental, w_a maps every positive root $\neq a$ upon a positive root. Applying (1.2) to a and $w_a(s)$, transform the resulting identity by ω_a, and rearrange the factors on the right such that the roots form an increasing sequence. Then by (1.6) we have the resired result.

(1.10) For any $r \in \Sigma$, we have $\omega_{-r}\omega_r = 1$.

Proof. Since

$$\omega_{-r} = \phi_{-r}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \phi_{-r}\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$$
$$= x_{-r}(1)x_r(-1)x_{-r}(1) = \phi_r\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right),$$

we have

$$\omega_{-r}\omega_r = \phi_r\left(\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)$$
$$= \phi_r\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = 1.$$

(1.11) If $r_1, \cdots, r_m \in \Sigma$ satisfy

$$(*) \qquad w_{r_1}\cdots w_{r_m} = 1,$$

then there exists $\chi \in X$ such that $\chi(s) = \eta_s$ for all $s \in \Sigma$, where η_s are the integers defined in (1.8) from $r_1, \cdots, r_m$.

Proof. Let

$$\omega = \omega_{r_1}\cdots\omega_{r_m}.$$

Then by (1.6) and the definition of η_s we have

$$\omega x_s(t)\omega^{-1} = x_s(\eta_s t)$$

for all $t \in K$. Applying the homomorphism $x \rightarrow \hat{x}$ to the above,

$$\hat{\omega}\hat{x}_s(t)\hat{\omega}^{-1} = \hat{x}_s(\eta_s t).$$

On the other hand, it is known ([2], Lemma 3, p. 37; Lemma 4, p. 49) that (*) implies that $\hat{\omega} = \hat{h}(\chi)$ for some $\chi \in X$. Then

$$\hat{h}(\chi)\hat{x}_s(t)\hat{h}(\chi)^{-1} = \hat{x}_s(\chi(s)t) = \hat{x}_s(\eta_s t).$$

Hence we have $\chi(s) = \eta_s$ for all $s \in \Sigma$.

From (1.8) and (1.11) we obtain

(1.12) If $r_1, \cdots, r_m \in \Sigma$ satisfy the condition (*) in (1.11), then for some $\chi \in X$ we have

$$\omega_{r_1}\cdots\omega_{r_m} = h(\chi).$$

Denote by $\mathfrak{U}$ (resp. $\mathfrak{V}$) the subgroup of G generated by the $x_r(t)$ with $r > 0$ (resp. $r < 0$), and by $\mathfrak{H}$ the group generated by all the $h(\chi)$, $\chi \in X$. For each $w \in W$ denote by $\mathfrak{U}_w$ the group generated by all the $x_r(t)$, $t \in K$, such that $r > 0$ and $w(r) < 0$. Also for each $w \in W$, choose once and for all roots $r_1, \cdots, r_m \in \Sigma$ such that

$$w = w_{r_1}\cdots w_{r_m}$$

and set

$$\omega(w) = \omega_{r_1}\cdots\omega_{r_m}.$$

Then we have the following fundamental proposition:

(1.13) Every element in G is written uniquely in the form $uh\omega(w)u'$, where $u \in \mathfrak{U}$, $h \in \mathfrak{H}$, $w \in W$, and $u' \in \mathfrak{U}_w$.

First we shall prove the uniqueness part of (1.13). Suppose $uh\omega(w)u' = u_1h_1\omega(w_1)u_1'$ with $u_1 \in \mathfrak{U}$, $h_1 \in \mathfrak{H}$, $w_1 \in W$, and $u_1' \in \mathfrak{U}_{w_1}$. Then $\hat{u}\hat{h}\hat{\omega}(w)\hat{u}' = \hat{u}_1\hat{h}_1\hat{\omega}(w_1)\hat{u}_1'$. Then by [2], Theorem 2, we have $\hat{u} = \hat{u}_1$, $\hat{h} = \hat{h}_1$, $\hat{w} = \hat{w}_1$, $\hat{u}' = \hat{u}_1'$. By (1.2) we can write u and u_1 in the form $\prod_r x_r(t_r)$, where r runs over all positive roots arranged as an increasing sequence and where $t_r \in K$. Then by [2], Lemma 6, p. 39, $\hat{u} = \hat{u}_1$ implies that t_r for u and u_1 coincide for all $r > 0$. Hence $u = u_1$ Similarly, $u' = u_1'$. Since $w = w_1$, we have $h = h'$ also. Thus the uniqueness part of (1.13) is proved.

Before continuing the proof of (1.13) we shall make a definition. For any element ω of the form

$$\omega = \omega_{r_1} \cdots \omega_{r_m} \tag{1.14}$$

define $\zeta(\omega)$ by

$$\zeta(\omega) = w_{r_1} \cdots w_{r_m}.$$

It can be easily seen from (1.6) and the uniqueness part of (1.13), above, that $\zeta(\omega)$ is independent of the mode of representing ω.

Now, a process of putting the given element x in G in the form of (1.13) is given in [2], p. 38-40. The properties (1.1)-(1.9) are sufficient to carry out the process. Since this process is needed later, we shall describe it in detail for the convenience of the reader. It consists of the three steps (1.15)-(1.17), below.

(1.15) *Step* 1. We express the given element x as $x_1x_2 \cdots x_n$, where each factor x_i is either of the form $x_{\pm a}(t)$ or of the form $\omega_{\pm a}$ with a fundamental root a.

This step may be divided into the following 2 parts:

(i) Write the given element x in the form $\prod_r x_r(t_r)$.

(ii) For each non-fundamental $r \in \Sigma$ appearing in (i), above, choose $w \in W$ and a fundamental root a such that $r = w(a)$; find fundamental roots $a_1, \cdots, a_m$ such that

$$w = w_{a_1} \cdots w_{a_m},$$

and replace $x_r(t)$ in (i) by

$$\omega_{a_1} \cdots \omega_{a_m} x_a(\pm t)\,\omega_{-a_m} \cdots \omega_{-a_1}.$$

(1.16) *Step* 2. We express the given element x in the form

$$x = uh\omega u' \tag{*}$$

where $u,\ u' \in \mathfrak{U},\ h \in \mathfrak{H}$ and ω is an element of the form given in (1.14).

This step is carried out as follows. Let $x = x_1 \cdots x_n$ as in (1.15), and set

$$y_0 = 1, y_1 = x_n, y_2 = x_{n-1}x_n, \cdots, y_n = x_1 \cdots x_n.$$

Then y_0 is trivially in the form (*). Suppose $y_i = uh\omega u'$ is in the form (*). If $y_{i+1} = x_a(t)y_i$ with a fundamental root a, then y_{i+1} is also in the form (*). If $y_{i+1} = \omega_{\pm a}y_i$ or if $y_{i+1} = x_{-a}(t)y_i$, then write u appearing in y_i in the form $u = u_1x_a(t_1)$, where u_1 is a product of some $x_r(t')$ with $r > 0,\ r \neq a$. Then by [2], Lemma 8, p. 40, y_{i+1} can be written in the form $u_2hv\omega u'$, where $v \in \phi_a(SL(2;K))$. Set $w = \zeta(\omega)$. Two possibilities arise: $w^{-1}(a) < 0$.

Case 1. $w^{-1}(a) > 0$. By [2], p. 34, write v as $v = x_a(t')h$ or $v = x_a(t')h\omega_a x_a(t'')$, where $h \in \mathfrak{H}$. Then it can be seen easily that y_{i+1} can be put in the form (*).

Case 2. $w^{-1}(a) < 0$. Use $\omega_1 = \omega_a\omega$ instead of ω. Set $w_1 = \zeta(\omega_1)$. Then $w_1(a) < 0$. Hence we are in case 1.

Thus, proceeding inductively, we can put $y_n = x$ in the form (*).

(1.17) *Step* 3. We finally express the given element x in the form specified in (1.13), starting from the expression $x = uh\omega u'$ obtained in (1.16). By making repeated use of (1.2), if necessary, we express $u' \in \mathfrak{U}$ as $u' = u_1u_2$, where u_1 is a product of $x_r(t)$ such that $r > 0,\ w(r) > 0$, where $w = \zeta(\omega)$, while $u_2 \in \mathfrak{U}_w$. Then by (1.5), (1.6), and (1.7), we can write $x = u_3h\omega u_2$ with $u_3 \in \mathfrak{U}$. Also, by (1.12), $\omega = h_1\omega(w)$ with $h_1 \in \mathfrak{H}$. Thus (1.13) is proved.

Now let x be any element in the kernel of the homomorphism $x \to \hat{x}$, and write $x = uh\omega(w)u'$ as in (1.13). Then arguing as in the proof of the uniqueness part of (1.13), one can show easily that $\hat{x} = 1$ implies $x = 1$. Hence the map $x \to \hat{x}$ is an isomorphism of G onto $\hat{G}$. Thus we have proved

THEOREM 1.18. *For any simple root system Σ and any field K, the Chevalley group G of type Σ over K is characterized by the properties* (1.1)-(1.8).[4]

The constants $C_{ij;r,s}$ and $\eta_{r,s}$ are not uniquely determined by Σ. If, however, we have, in the simple Lie algebra of type Σ over the complex number field, a set $\{X_r \mid r \in \Sigma\}$ of root vectors which satisfies the conditions in Theorem 1 of [2], then we can obtain a set of the above constants by setting $x_r(t) = \exp(t \operatorname{ad} X_r)$ and by the relations (1.2) and (1.6). The constants $\eta_{r,s}$ can actually be defined by ([2], p. 36)

---

[4] For another characterization of Chevalley groups by generators and defining relations, see a forthcoming book by J. Tits.

(1.19) $$\omega_r X_s = \eta_{r,s} X_{w_r(s)}.$$

We have

(1.20) $$\eta_{r,r} = -1, \quad \eta_{r,-s} = \eta_{r,s}, \quad \eta_{-r,s} = \eta_{r,w_r(s)},$$

the first of which follows from (1.19) and the relation $\omega_r = x_r(1)x_{-r}(-1)x_r(1)$, the second from [2], p. 36, and the third from (1.9). Also from (1.9) we have

(1.21) If $r, s \in \Sigma$ are distinct, and if none of $r+s$, $r-s$ are in Σ, then $\eta_{r,s} = 1$.

For $r, s \in \Sigma$ such that $r+s \in \Sigma$, define the number $N_{r,s}$ by $[X_r, X_s] = N_{r,s} X_{r+s}$. Then from (1.19) we have

(1.22) If $r, s \in \Sigma$ and if $\pm r$, $\pm s$, $\pm(r+s)$ are the only linear combinations of r, s which are in Σ, then $\eta_{r,s} = N_{r,s}$.

(1.23) For any $r, s, u \in \Sigma$ such that $s+u \in \Sigma$, we have

$$\eta_{r,s}\eta_{r,u}N_{w_r(s),w_r(u)} = \eta_{r,s+u}N_{s,u}.$$

2. The root system of type (G_2). The root system Σ of type (G_2) can be given as

$$\Sigma = \{\pm \xi_i, \xi_i - \xi_j \mid i, j = 1, 2, 3; i \neq j\},$$

where $\xi_1 + \xi_2 + \xi_3 = 0$. The Weyl group W of Σ is of order 12, and consists of elements w such that $w(\xi_i) = e\xi_{\pi(i)}$, $i = 1, 2, 3$, and $e = \pm 1$, and where π is a permutation of 1, 2, 3. We shall write $w = (e, \pi)$. Then $w_r = (1, (ij))$ for $r = \xi_i - \xi_j$, where (ij) denotes the transposition of i and j, and $w_r = (-1, (i'i''))$ for $r = \pm \xi_i$, where i, i', i'' is a permutation of 1, 2, 3.

The relationship between the roots and the action of W on Σ can be seen easily in Fig. 1, where Σ is represented as a system of vectors on a Euclidean plane. The element $w_r \in W$ is nothing but the symmetry with respect to the line which passes through the origin and which is perpendicular to the vector representing the root $r \in \Sigma$. The function $\lambda(r)$ on Σ defined by

$$\lambda(\pm \xi_i) = 1, \qquad \lambda(\xi_i - \xi_j) = 3$$

for all $i, j = 1, 2, 3$; $i \neq j$, has a clear meaning in Fig. 1.

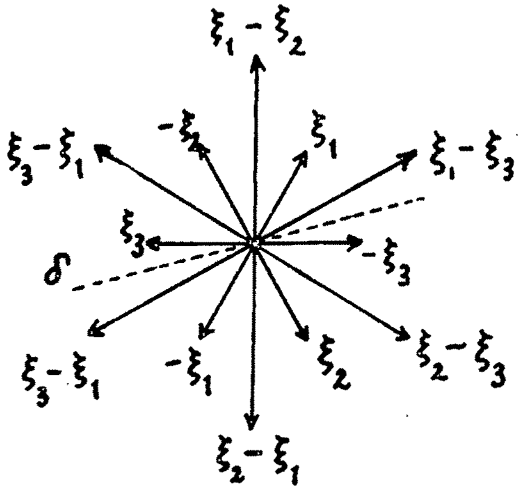

FIGURE 1.

Since $w_r(s) = s - s(r)r$, one can see easily that

$$(r, s) = \tfrac{1}{2}\lambda(s)r(s) \tag{2.1}$$

coincides with the Euclidean inner product of the vectors $r, s \in \Sigma$.

Denote by P, as in Section 1, the additive group generated by Σ, and define a homomorphism $\psi\colon P \to P$ by

$$\psi(\xi_1) = \xi_2 - \xi_3, \qquad \psi(\xi_2) = \xi_1 - \xi_2. \tag{2.2}$$

Then one can see easily that

$$\psi(r) = \lambda(r)\bar{r} \tag{2.3}$$

holds for all $r \in \Sigma$, where $r \to \bar{r}$ is a permutation of order 2 of Σ such that

$$\overline{-r} = -\bar{r}, \qquad \lambda(r)\lambda(\bar{r}) = 3 \tag{2.4}$$

for all $r \in \Sigma$. From the definition of ψ, it is clear that $\psi = \sqrt{3}\,\psi_\delta$, where ψ_δ is the symmetry with respect to the line δ bisecting the angle between $\xi_1 - \xi_3$ and $-\xi_3$ in Fig. 1.[5] Hence $(\psi(r), \psi(s)) = 3(r, s)$, which yields, by (2.1), (2.3), and (2.4),

$$\lambda(r)\bar{r}(\bar{s}) = \lambda(s)r(s) \tag{2.5}$$

for all r, s in Σ.

---

[5] The idea of considering the line δ in connection with the map ψ was suggested to the author by J. Tits.

Applying ψ to $w_r(s) = s - s(r)r$, we get

$$\psi(w_r(s)) = \lambda(s)\bar{s} - \lambda(r)s(r)\bar{r} = \lambda(s)\bar{s} - \lambda(s)\bar{s}(\bar{r})\bar{r}$$

by (2.5). Since $\lambda(w_r(s)) = \lambda(s)$, we have from the above

$$\overline{w_r(s)} = w_{\bar{r}}(\bar{s}) \tag{2.6}$$

for all $r, s \in \Sigma$. For each $w \in W$, define a permutation $\bar{w}$ of Σ by

$$\bar{w}(\bar{s}) = \overline{w(s)}. \tag{2.7}$$

Then from (2.6) we have immediately

(2.8) The map $w \to \bar{w}$ is an automorphism of the Weyl group W such that $\bar{w}_r = w_{\bar{r}}$ for all $r \in \Sigma$.

We shall consider elements invariant under the automorphism $w \to \bar{w}$. Suppose $w = (e, \pi)$ satisfies $\bar{w} = w$. Then from (2.7) we obtain

$$\bar{\xi}_{\pi(1)} = \xi_{\pi(2)} - \xi_{\pi(3)}, \ \bar{\xi}_{\pi(2)} = \xi_{\pi(1)} - \xi_{\pi(2)}$$

from which one can deduce easily that π is the identity permutation. Hence

(2.9) If $\bar{w} = w$, then $w = 1$ or $w = w_0$, where w_0 is defined by $w_0(r) = -r$ for all $r \in \Sigma$.

3. Chevalley groups of type (G_2). We shall determine a set of the constants $C_{ij;r,s}$ and $\eta_{r,s}$ for the root system Σ of type (G_2). The simple Lie algebra $\mathfrak{g}$ of type (G_2) has a basis

$$X_{ij}, \quad X_{i0}, \quad X_{0i}, \quad H_{ij}, \tag{3.1}$$

where $i, j = 1, 2, 3$; $i \neq j$, and where

$$H_{ij} + H_{ji} = 0; \quad H_{12} + H_{23} + H_{31} = 0. \tag{3.2}$$

The multiplication table is

$$\begin{array}{ll} [X_{ij}X_{jk}] = X_{ik}, & [X_{i0}X_{0j}] = 3X_{ij}, \\ [X_{0i}X_{ij}] = X_{0j}, & [X_{ij}X_{j0}] = X_{i0}, \\ [X_{i0}X_{j0}] = 2(ijk)X_{0k}, & [X_{0i}X_{0j}] = -2(ijk)X_{k0}, \\ [X_{ij}X_{ji}] = H_{ij}, & [X_{i0}X_{0i}] = H_{ij} + H_{ik}, \\ [X_{i0}H_{ij}] = -X_{i0}, & [X_{0i}H_{ij}] = X_{0i}, \\ [X_{ij}H_{ij}] = -2X_{ij}, & [X_{ij}H_{jk}] = [X_{ij}H_{ki}] = X_{ij}, \end{array} \tag{3.3}$$

where i, j, k run over distinct values of 1, 2, 3, and where $(ijk) = 1$ or -1 according as i, j, k is an even or odd permutation of 1, 2, 3. All the other products of basis element which cannot be computed trivially from (3.2) and (3.3) are zero.

The elements H_{ij} span a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$, and X_{ij}, X_{i0}, X_{0i} are root vectors with respect to $\mathfrak{h}$, corresponding respectively to the roots $\xi_i - \xi_j$, ξ_i, $-\xi_i$ given in Section 2. These root vectors satisfy the conditions in Theorem 1 of [2], and hence the table (3.3) can be used to compute a set of the constants $C_{ij;r,s}$ and $\eta_{r,s}$.

The constants $\eta_{r,s}$ can be computed easily by (1.19)-(1.23), and by the fact that any even permutation of i, j, k leaves the table (3.3) invariant. The result of the computation is give in table (3.4).

(3.4) The table of $\eta_{r,s}$

s r	ξ_1	ξ_2	ξ_3	$\xi_1 - \xi_2$	$\xi_2 - \xi_3$	$\xi_3 - \xi_1$
ξ_1	-1	-1	1	-1	1	1
ξ_2	1	-1	-1	1	-1	1
ξ_3	-1	1	-1	1	1	-1
$\xi_1 - \xi_2$	-1	1	1	-1	1	-1
$\xi_2 - \xi_3$	1	-1	1	-1	-1	1
$\xi_3 - \xi_1$	1	1	-1	1	-1	-1

All the other value of $\eta_{r,s}$ which are not found in (3.4) can readily be supplied by (1.20).

As an immediate application of (3.4) and (1.20), we can verify the equality

$$\eta_{\bar{r},\bar{s}} = \eta_{r,s} \tag{3.5}$$

for all $r, s \in \Sigma$, where $r \to \bar{r}$ is the map defined in Section 2. Also, using (3.4) and (1.20) we can show that

$$\omega_0 = \omega_{\xi_1}\omega_{\xi_2-\xi_3} = \omega_{\xi_2-\xi_3}\omega_{\xi_1}$$

satisfies

$$\omega_0 x_r(t)\,\omega_0^{-1} = x_{-r}(-t) \tag{3.6}$$

for all $r \in \Sigma$ and $t \in K$, and hence

$$\omega_0^2 = 1. \tag{3.7}$$

Similarly, using (3.4) and the symmetry of the table (3.3), and noting that there can be only one element $\omega_0 \in G$ satisfying (3.6), one can show that

$$\begin{aligned} \omega_0 &= \omega_{\xi_i}\omega_{\xi_j-\xi_k} = \omega_{\xi_j-\xi_k}\omega_{\xi_i} \\ &= \omega_{-\xi_k}\omega_{\xi_j-\xi_i} = \omega_{\xi_j-\xi_i}\omega_{-\xi_k} \end{aligned} \tag{3.8}$$

holds for any even permutation i, j, k of 1, 2, 3.

Now, in order to consider the constants $C_{ij;r,s}$, we shall fix an order in Σ. Set $a=\xi_2$, $b=\xi_1-\xi_2$. Then all the roots are $\pm a$, $\pm b$, $\pm(a+b)$, $\pm(2a+b)$, $\pm(3a+b)$, $\pm(3a+2b)$. We can regard $a, b, a+b, \cdots$ to be positive. Then the fundamental roots are a and b. For the map $r\rightarrow\bar{r}$ defined in Section 2, we have

$$\bar{a}=b, \quad (a+b)^{-}=3a+b, \quad (2a+b)^{-}=3a+2b. \tag{3.9}$$

Now, the constants $C_{1j;r,s}$ and $C_{i1;r,s}$ can be computed easily from (3.3) using the formulas given in [2], p. 36, but $C_{3,2;a,b}$ must be computed directly from (3.3). We shall express the results of our computation in the following form:

$$\begin{aligned}
(x_a(t), x_b(u)) &= x_{a+b}(-tu)x_{2a+b}(-t^2u)x_{3a+b}(t^3u)x_{3a+2b}(-2t^3u^2),\\
(x_a(t), x_{a+b}(u)) &= x_{2a+b}(-2tu)x_{3a+b}(3t^2u)x_{3a+2b}(3tu^2),\\
(x_a(t), x_{2a+b}(u)) &= x_{3a+b}(3tu),\\
(x_b(t), x_{3a+b}(u)) &= x_{3a+2b}(tu),\\
(x_{a+b}(t), x_{2a+b}(u)) &= x_{3a+2b}(3tu),
\end{aligned} \tag{3.10}$$

where $(x,y)=x^{-1}y^{-1}xy$. For all the other pairs of positive roots r, s, we have $(x_r(t), x_s(u))=1$.

4. An automorphism of G.

In this section we assume that K is a perfect field of characteristic 3, and that $t\rightarrow t^{\theta}$ is an automorphism of K.

Let Σ be the root system of type (G_2). Using the notation introduced in Section 2, define $\bar{\chi}$ for each $\chi\in X$, by

$$\bar{\chi}(r)=\chi(\psi(r))^{\theta}=\chi(\bar{r})^{\lambda(r)\theta}. \tag{4.1}$$

Then one can show easily by (4.1) and (2.5) that

$$\bar{\chi}_{r,z}=\chi_{\bar{r},z}{}^{\lambda(\bar{r})\theta} \tag{4.2}$$

for all $r\in\Sigma$ and $z\in K^*$.

Let G be the Chevalley group of type (G_2) over K. Set

$$\bar{x}_r(t)=x_{\bar{r}}(t^{\lambda(\bar{r})\theta}). \tag{4.3}$$

Define the homomorphism $\bar{\phi}_r: SL(2;K)\rightarrow G$ by

$$\bar{\phi}_r\begin{pmatrix} t_1 & t_2\\ t_3 & t_4\end{pmatrix}=\phi_{\bar{r}}\begin{pmatrix} t_1{}^{\lambda(\bar{r})\theta} & t_3{}^{\lambda(\bar{r})\theta}\\ t_2{}^{\lambda(\bar{r})\theta} & t_4{}^{\lambda(\bar{r})\theta}\end{pmatrix}. \tag{4.4}$$

Define the homomorphism $\bar{h}: X\rightarrow G$ by

$$\bar{h}(\chi)=h(\bar{\chi}). \tag{4.5}$$

We shall show that we can replace $x_r(t)$, ϕ_r, h in (1.1)-(1.8) by $\bar{x}_r(t)$, $\bar{\phi}_r$, $\bar{h}$, respectively, without losing the validity of the statements. Denote by (1.n′) the statement obtained from (1.n) by the replacement. Then (1.1′) is clear. (1.3′) follows easily from (4.3), (4.4) and (2.4). (1.4′) follows from (1.4), (4.2), and (4.4). (1.5′) follows from (1.5), (4.1), and (4.3). As for (1.6′), ω_r is replaced by $\omega_{\bar{r}}$, since

$$\bar{\phi}_r\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \phi_{\bar{r}}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \omega_{\bar{r}}. \tag{4.6}$$

Then (1.6′) follows from (1.6), (4.3), (3.5), (2.6), and the fact that $\lambda(w(r)) = \lambda(r)$ for all $w \in W$ and $r \in \Sigma$. As for (1.7′), ω is, by (4.6), replaced by

$$\bar{\omega} = \omega_{\bar{r}_1} \cdots \omega_{\bar{r}_m}.$$

Hence, by (1.7) and (2.8), we have $\bar{\omega}\bar{h}(\chi)\bar{\omega}^{-1} = h(\chi_1)$, where χ_1 is defined by $\chi_1(s) = \bar{\chi}(\bar{w}^{-1}(s))$. Then, by (4.1),

$$\begin{aligned} \chi_1(s) &= \chi((\bar{w}^{-1}(s))^{-})^{\lambda(\bar{w}^{-1}(s))\theta} \\ &= \chi(w^{-1}(\bar{s}))^{\lambda(s)\theta} = \overline{\chi'}(s), \end{aligned}$$

where r^{-} denotes $\bar{r}$ for $r \in \Sigma$. Therefore, $\chi_1 = \overline{\chi'}$. Now, (1.7′) follows from (4.5). Also it can be seen that (1.8′) follows from (1.8), (2.8), (3.5), and (4.1). It remains to prove (1.2′). Since K is of characteristic 3, (3.10) now becomes

$$\begin{aligned} (x_a(t), x_b(u)) &= x_{a+b}(-tu)x_{2a+b}(-t^2u)x_{3a+b}(t^3u)x_{3a+2b}(t^3u^2), \\ (x_a(t), x_{a+b}(u)) &= x_{2a+b}(tu), \\ (x_b(t), x_{3a+b}(u)) &= x_{3a+2b}(tu), \end{aligned} \tag{4.7}$$

and all the other commutators of the form $(x_r(t), x_s(u))$, where $r > 0$, $s > 0$, are 1. Since the set of pairs $\{a, b\}$, $\{a, a+b\}$, $\{b, 3a+b\}$ is invariant under the map $\{r, s\} \to \{\bar{r}, \bar{s}\}$, it is clear, in view of (4.3), that $(x_r(t), x_s(u)) = 1$, $r > 0$, $s > 0$, implies $(\bar{x}_r(t), \bar{x}_s(u)) = 1$. Since

$$\begin{aligned} \lambda(a) = \lambda(a+b) = \lambda(2a+b) = 1, \\ \lambda(b) = \lambda(3a+b) = \lambda(3a+2b) = 3, \end{aligned}$$

we have by (3.9)

$$\begin{aligned} (\bar{x}_a(t), \bar{x}_b(u)) &= (x_b(t^{3\theta}), x_a(u^{\theta})) = (x_a(u^{\theta}), x_b(t^{3\theta}))^{-1} \\ &= x_{3a+2b}(-u^{3\theta}t^{6\theta})x_{3a+b}(-u^{3\theta}t^{3\theta})x_{2a+b}(u^{2\theta}t^{3\theta})x_{a+b}(u^{\theta}t^{3\theta}) \\ &= x_{3a+b}((-tu)^{3\theta})x_{3a+2b}((-t^2u)^{3\theta})x_{a+b}((t^3u)^{\theta})x_{2a+b}((t^3u^2)^{\theta}) \\ &= \bar{x}_{a+b}(-tu)\bar{x}_{2a+b}(-t^2u)\bar{x}_{3a+b}(t^3u)\bar{x}_{3a+2b}(t^3u^2). \end{aligned}$$

Thus it is shown that the first equation of (4.7) remains valid under the replacement $x_r(t) \rightarrow \bar{x}_r(t)$. Similarly the rest of (1.2′) can be proved. Thus we have proved (1.1′)-(1.8′). Then from Theorem 1.18 and the simplicity of G, we obtain

THEOREM 4.8. *If K is a perfect field of characteristic 3, and if $t \rightarrow t^\theta$ is an automorphism of K, then the Chevalley group of type (G_2) over K admits an automorphism $x \rightarrow x^\sigma$ such that*

$$x_r(t)^\sigma = x_{\bar{r}}(t^{\lambda(\bar{r})\theta})$$

for all $r \in \Sigma$ and $t \in K$. The automorphism σ maps $\mathfrak{U}$, $\mathfrak{H}$, $\mathfrak{W}$ onto themselves, respectively, and

$$h(\chi)^\sigma = h(\bar{\chi}), \qquad \omega_r{}^\sigma = \omega_{\bar{r}}$$

for all $\chi \in X$ and $r \in \Sigma$, where $\bar{\chi}$ is defined by (4.1).[6]

5. Invariant elements. From now on we assume that K is a perfect field of characteristic 3, and that the automorphism θ satisfies

$$(5.1) \qquad 3\theta^2 = 1,$$

the right hand side of (5.1) being the identity automorphism.[7]

Before considering the group G, we shall derive a few properties of the field K from (5.1). Since

$$(z^{3\theta+1})^{3\theta-1} = z^2, \qquad (z^{3\theta-2})^{3\theta+2} = z^{-1},$$

we have

(5.2) Every element in K^{*2} is of the form $z^{3\theta-1}$ with $z \in K^*$.

(5.3) Every element in K^* is of the form $z^{3\theta-2}$ and also of the form $z^{3\theta+2}$.

(5.4)[8] -1 has no square root in K.

Proof. Suppose $z^2 = -1$. Then $(z^\theta)^2 = -1$, $z^\theta = \pm z$, and hence

$$z = (z^{3\theta})^\theta = (-z^\theta)^\theta = (\mp z)^\theta = -z,$$

but this is impossible.

---

[6] After the completion of earlier versions of this paper and [9], the author learned from Tits that the existence of the automorphism σ was already mentioned in [6], p. 282. See also R. Steinberg [8].

[7] It was discovered by Tits that K need not be assumed to be perfect if one considers an endomorphism η, instead of θ, of K such that $\eta^2 = 3$. For the details of this, see [7].

[8] This lemma was pointed out to the author by R. Steinberg and J. Tits, independently. The proof given here is due to Tits.

An element x in G will be said to be *σ-invariant* if $x^\sigma = x$. First we shall consider σ-invariant elements in $\mathfrak{U}$. Suppose

$$x = x_a(t_{10})x_b(t_{01})x_{a+b}(t_{11})x_{2a+b}(t_{21})x_{3a+b}(t_{31})x_{3a+2b}(t_{32})$$

is σ-invariant. We have

$$x^\sigma = x_b(t_{10}{}^{3\theta})x_a(t_{01}{}^{\theta})x_{3a+b}(t_{11}{}^{3\theta})x_{3a+2b}(t_{21}{}^{3\theta})x_{a+b}(t_{31}{}^{\theta})x_{2a+b}(t_{32}{}^{\theta}).$$

By (4.7), the right hand side of the above can be changed into the form $x_a(s_{10})x_b(s_{01})\cdots x_{3a+2b}(s_{32})$. Then comparing with x, we get

$$\begin{gathered} t_{01}{}^{\theta} = t_{10},\ t_{31}{}^{\theta} + t_{01}{}^{\theta}t_{10}{}^{3\theta} = t_{11},\ t_{32}{}^{\theta} + t_{01}{}^{2\theta}t_{10}{}^{3\theta} = t_{21}, \\ t_{10}{}^{3\theta} = t_{01},\ t_{11}{}^{3\theta} - t_{01}{}^{3\theta}t_{10}{}^{3\theta} = t_{31},\ t_{21}{}^{3\theta} - t_{01}{}^{3\theta}t_{10}{}^{6\theta} = t_{32}. \end{gathered}$$

By (5.1), the equations in the first row, above, are equivalent to the equations in the second row. Hence if we set $t_{01} = t$, $t_{31} = u$, $t_{32} = v$, then $x = \alpha(t)\beta(u)\gamma(v)$, where

$$\begin{aligned} \alpha(t) &= x_a(t^\theta)x_b(t)x_{a+b}(t^{\theta+1})x_{2a+b}(t^{2\theta+1}), \\ \beta(t) &= x_{a+b}(t^\theta)x_{3a+b}(t), \\ \gamma(t) &= x_{2a+b}(t^\theta)x_{3a+2b}(t). \end{aligned}$$

Hence, by [2], Lemma 6, p. 39, we have

(5.5) The group $\mathfrak{U}^1$ of σ-invariant elements in $\mathfrak{U}$ contains $\alpha(t), \beta(t)$, $\gamma(t)$ for all $t \in K$. Every element in $\mathfrak{U}^1$ is written uniquely as $\alpha(t)\beta(u)\gamma(v)$ with t, u, $v \in K$.

By using (4.7) one can show easily

$$\begin{aligned} &\alpha(t)\alpha(u) = \alpha(t+u)\beta(-tu^{3\theta})\gamma(-t^2u^{3\theta} + tu^{3\theta+1}), \\ &\beta(t)\alpha(u) = \alpha(u)\beta(t)\gamma(-tu),\ \beta(t)\beta(u) = \beta(t+u), \\ &\gamma(t)\alpha(u) = \alpha(u)\gamma(t),\ \gamma(t)\beta(u) = \beta(u)\gamma(t), \\ &\gamma(t)\gamma(u) = \gamma(t+u). \end{aligned} \tag{5.6}$$

It can be shown easily from the above that the group $\mathfrak{U}^1$ is generated by the elements $\alpha(t)$, $t \in K$.

Before considering σ-invariant elements in $\mathfrak{B}$, we remark that the element ω_0 given in (3.8) can be written

$$\omega_0 = \omega_{a+b}\omega_{3a+b} = \omega_{3a+b}\omega_{a+b} \tag{5.7}$$

and hence is σ-invariant by (3.9) and Theorem 4.8. Now define the elements $\alpha'(t)$, $\beta'(t)$, $\gamma'(t)$ by

$$\begin{aligned}\alpha'(-t) &= \omega_0\alpha(t)\omega_0^{-1}\\ &= x_{-a}(-t^{\theta})x_{-b}(-t)x_{-(a+b)}(-t^{\theta+1})x_{-(2a+b)}(-t^{2\theta+1}),\\ \beta'(-t) &= \omega_0\beta(t)\omega^{-1} = x_{-(a+b)}(-t^{\theta})x_{-(3a+b)}(-t),\\ \gamma'(-t) &= \omega_0\gamma(t)\omega_0^{-1} = x_{-(2a+b)}(-t^{\theta})x_{-(3a+2b)}(-t).\end{aligned}$$

Then from (5.5) and the σ-invariance of ω_0 we have

(5.8) The group $\mathfrak{B}^1$ of σ-invariant elements in $\mathfrak{B}$ contains $\alpha'(t), \beta(t), \gamma'(t)$ for all $t \in K$; every element in $\mathfrak{B}^1$ is written uniquely in the form $\alpha'(t)\beta'(u)\gamma'(v)$ with $t, u, v \in K$.

Denote by G^1 the group generated by $\mathfrak{U}^1$ and $\mathfrak{B}^1$. Since

$$\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$$

and since any one of $x_{-(a+b)}(t_1)$, $x_{a+b}(t_2)$ commute with any one of $x_{3a+b}(t_3)$, $x_{-(3a+b)}(t_4)$, we have from (5.7)

$$(5.9)\qquad \omega_0 = \beta(1)\beta'(-1)\beta(1) \in G^1.$$

Now we shall consider σ-invariant elements in $\mathfrak{H}$. We have $h(\chi)^{\sigma} = h(\bar{\chi})$. Since a and b generate P, χ is determined by $\chi(a)$ and $\chi(b)$. From (4.1) we get

$$(5.10)\qquad \bar{\chi}(a) = \chi(b)^{\theta},\ \bar{\chi}(b) = \chi(a)^{3\theta}.$$

Hence we have

(5.11) $h(\chi)$ is σ-invariant if and only if $\chi(a) = \chi(b)^{\theta}$.

By (1.5) and the definition of the elements $\alpha(t), \cdots$, we have

(5.12) If $h(\chi)$ is σ-invariant, then

$$\begin{aligned}&h(\chi)\alpha(t)h(\chi)^{-1} = \alpha(\chi(b)t), && h(\chi)\alpha'(t)h(\chi)^{-1} = \alpha'(\chi(b)^{-1}t),\\ &h(\chi)\beta(t)h(\chi)^{-1} = \beta(\chi(b)^{3\theta+1}t), && h(\chi)\beta'(t)h(\chi)^{-1} = \beta'(\chi(b)^{-3\theta-1}t),\\ &h(\chi)\gamma(t)h(\chi)^{-1} = \gamma(\chi(b)^{3\theta+2}t), && h(\chi)\gamma'(t)h(\chi)^{-1} = \gamma'(\chi(b)^{-3\theta-2}t).\end{aligned}$$

Denote by $\mathfrak{H}^1$ the group of all σ-invariant elements in $\mathfrak{H}$, and by $\mathfrak{H}^2$ the subgroup of $\mathfrak{H}^1$ consisting of all σ-invariant $h(\chi)$ such that $\chi(b) = z^{3\theta-1}$ with some $z \in K^*$. Note that some elements, for instance -1, in K cannot be written in the form $z^{3\theta-1}$. Since

$$\begin{pmatrix} z & 0\\ 0 & z^{-1}\end{pmatrix} = \begin{pmatrix} 1 & 0\\ z^{-1}-1 & 1\end{pmatrix}\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 1\\ z-1 & 1\end{pmatrix}\begin{pmatrix} 1 & -z^{-1}\\ 0 & 1\end{pmatrix}$$

and since any one of $x_{a+b}(t_1)$, $x_{-(a+b)}(t_2)$ commute with any one of $x_{3a+b}(t_3)$, $x_{-(3a+b)}(t_4)$, we have

$$\beta'(z^{-1}-1)\beta(1)\beta'(z-1)\beta(-z^{-1})$$

$$=\phi_{a+b}\begin{pmatrix} z^{\theta} & 0 \\ 0 & z^{-\theta} \end{pmatrix}\phi_{3a+b}\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}=h(\chi_{a+b,z^{\theta}})h(\chi_{3a+b,z}).$$

Set

$$\chi=\chi_{a+b,z^{\theta}}\chi_{3a+b,z}.$$

Then it follows from the above that $h(\chi)\in G^1$. We have

$$\chi(b)=z^{b(a+b)\theta+b(3a+b)}=z^{3\theta-1}.$$

Since z is an arbitrary element in K^*, we have

$$\mathfrak{H}^2\subseteq G^1. \tag{5.13}$$

Now we shall determine all σ-invariant elements in G by (1.13). In view of (3.6), we can assume, for the w_0 given in (2.9), that

$$\omega(w_0)=\omega_0. \tag{5.14}$$

By (1.13) we can write any element x in G in the form $x=uh(\chi)\omega(w)u_1$, where $u\in\mathfrak{U}$ and u_1 is a product of elements of the form $x_r(t)$ with $r>0$, $w(r)<0$. We have $x^{\sigma}=u^{\sigma}h(\bar{\chi})\omega(w)^{\sigma}u_1^{\sigma}$. If

$$\omega(w)=\omega_{r_1}\cdots\omega_{r_m}$$

then by Theorem 4.8 we have

$$\omega(w)^{\sigma}=\omega_{\bar{r}_1}\cdots\omega_{\bar{r}_m}$$

and hence by (1.12) and (2.7) we can write $\omega(w)^{\sigma}=h(\chi_1)\omega(\bar{w})$. Then

$$x^{\sigma}=u^{\sigma}h(\bar{\chi}\chi_1)\omega(\bar{w})u_1^{\sigma}. \tag{5.15}$$

Here u_1^{σ} is a product of elements of the form $x_r(t)$, $r>0$, $w(r)<0$. We have $\bar{r}>0$, and $\bar{w}(\bar{r})=\overline{w(r)}<0$ by (2.7). Hence the expression for x^{σ} given in (5.15) is exactly in the form specified in (1.13). Assume that x is σ-invariant. Then $x=x^{\sigma}$, and the uniqueness in (1.13) implies

$$u=u^{\sigma},\quad \chi=\bar{\chi}\chi_1,\quad w=\bar{w},\quad u_1=u_1^{\sigma}.$$

Then by (2.9) we have $w=1$ or $w=w_0$. Then, since we can assume $\omega(1)=1$, we have from (5.14) $\omega(w)^{\sigma}=\omega(w)$, and hence $h(\chi_1)=1$, $\chi_1=1$. Hence $\chi=\bar{\chi}$ and $h(\chi)$ is σ-invariant. Thus we have proved

(5.16) Any σ-invariant element x in G is written uniquely in the form $x=uh(\chi)\omega u_1$, where: $u\in\mathfrak{U}^1$; $\bar{\chi}=\chi$; $\omega=1$ or ω_0; $u_1=1$ if $\omega=1$, but u_1 is an arbitrary element in $\mathfrak{U}^1$ if $\omega=\omega_0$.

The form of x given in (5.16), above, will be called the *canonical form* of x.

6. Some identities. We shall compute the canonical forms for $\alpha'(t)$ and $\gamma'(t)$, by following, more or less, the steps (1.15)-(1.17). The results are crucial, as will be seen later, in the discussion of the structure of G^1. Note that our assumption on the field K is the same as in the preceding section.

(6.1) If $t \in K^*$, then

$$\alpha'(t) = \gamma(t^{-(3\theta+2)})\beta(t^{-(3\theta+1)})\alpha(t^{-1})^{-1}h(\chi)\omega_0\,\alpha(t^{-1})\beta(t^{-(3\theta+1)})\gamma(t^{-(3\theta+2)}),$$

where χ is defined by $\chi(a) = -t^{-2\theta}$, $\chi(b) = -t^{-2}$.

Proof. We have

$$\alpha'(t) = x_{-a}(t^{\theta})x_{-b}(t)x_{-(a+b)}(-t^{\theta+1})x_{-(2a+b)}(t^{2\theta+1}).$$

By applying ϕ_{2a+b} to

$$(6.2) \qquad \begin{pmatrix}1 & 0\\ u & 1\end{pmatrix} = \begin{pmatrix}1 & u^{-1}\\ 0 & 1\end{pmatrix}\begin{pmatrix}-u^{-1} & 0\\ 0 & -u\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}1 & u^{-1}\\ 0 & 1\end{pmatrix}$$

we obtain

$$x_{-(2a+b)}(t^{2\theta+1}) = x_{2a+b}(t^{-(2\theta+1)})h(\chi_1)\omega_{2a+b}x_{2a+b}(t^{-(2\theta+1)}),$$

where

$$\chi_1 = \chi_{2a+b,-t^{-(2\theta+1)}}.$$

By transforming the second equation of (4.7) by ω_{a+b}, we obtain

$$x_{-(a+b)}(-t^{\theta+1})x_{2a+b}(t^{-(2\theta+1)}) = x_{2a+b}(t^{-(2\theta+1)})x_a(t^{-\theta})x_{-(a+b)}(-t^{\theta+1}).$$

Hence we have

$$\begin{aligned}\alpha'(t) &= x_{-a}(t^{\theta})x_{2a+b}(t^{-(2\theta+1)})x_a(t^{-\theta})x_{-b}(t)x_{-(a+b)}(-t^{\theta+1})\\ &\qquad \cdot h(\chi_1)\omega_{2a+b}x_{2a+b}(t^{-(2\theta+1)})\\ &= x_{2a+b}(t^{-(2\theta+1)})x_{a+b}(t^{-(\theta+1)})x_{-a}(t^{\theta})x_a(t^{-\theta})x_b(t^{-1})h(\chi_2)\\ &\qquad \cdot \omega_{-b}x_b(t^{-1})h(\chi_1)\omega_{2a+b}x_{2a+b}(t^{-(2\theta+1)}),\end{aligned}$$

where

$$\chi_2 = \chi_{b,t^{-1}}$$

since, by transforming the second equation of (4.7) by ω_a, we obtain

$$x_{-a}(t^{\theta})x_{2a+b}(t^{-(2\theta+1)}) = x_{2a+b}(t^{-(2\theta+1)})x_{a+b}(t^{-(\theta+1)})x_{-a}(t^{\theta}).$$

Now, by applying ϕ_a to

$$\begin{pmatrix}1 & 0\\ u & 1\end{pmatrix}\begin{pmatrix}1 & u^{-1}\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & -u^{-1}\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ -u & 1\end{pmatrix}$$

we obtain

$$x_{-a}(t^{\theta})x_a(t^{-\theta}) = x_a(-t^{-\theta})h(\chi_3)x_{-a}(-t^{\theta}),$$

where

$$\chi_3 = \chi_{a,-1}.$$

Hence we have from the above

$$\begin{aligned}\alpha'(t) &= x_{2a+b}(t^{-(2\theta+1)})x_{a+b}(t^{-(\theta+1)})x_a(-t^{-\theta})h(\chi_3)x_b(t^{-1})x_{-a}(-t^{\theta}) \\ &\qquad \cdot h(\chi_2)\omega_{-b}x_b(t^{-1})x_{-(a+b)}(-t^{\theta+1})h(\chi_1)\omega_{2a+b}x_{2a+b}(t^{-(2\theta+1)}) \\ &= x_{2a+b}(t^{-(2\theta+1)})x_{a+b}(t^{-(\theta+1)})x_a(-t^{-\theta})x_b(-t^{-1})h(\chi_3)\omega_0 x_a(t^{\theta}) \\ &\qquad \cdot h(\chi_2)^{-1}x_b(t^{-1})x_a(t^{\theta+1})h(\chi_1 \circ w_{2a+b})x_{2a+b}(t^{-(2\theta+1)}),\end{aligned}$$

since $\omega_{-b}\omega_{2a+b} = \omega_0$ by (3.8). Since

$$\begin{aligned}& x_a(t^{\theta})h(\chi_2)^{-1}x_b(t^{-1})x_a(t^{\theta+1})h(\chi_1 \circ w_{2a+b}) \\ &\quad = h(\chi_2)^{-1}h(\chi_1 \circ w_{2a+b})x_a(t^{-\theta})x_b(t^{-1})x_{a+b}(-t^{-(\theta+1)})x_{2a+b}(t^{-(2\theta+1)}) \\ &\qquad\qquad \cdot x_{3a+b}(t^{-(3\theta+1)})x_{3a+2b}(t^{-(3\theta+2)}),\end{aligned}$$

we have

$$\begin{aligned}\alpha'(t) &= x_{2a+b}(t^{-2(\theta+1)})x_{a+b}(t^{-(\theta+1)})x_a(-t^{-\theta})x_b(-t^{-1})h(\chi)\omega_0 \\ &\qquad \cdot \alpha(t^{-1})\beta(t^{-(3\theta+1)})\gamma(t^{-(3\theta+2)}); \\ \chi &= \chi_3\chi_2(\chi_1 \circ w_{2a+b})^{-1}.\end{aligned}$$

From this one can derive (6.1) easily.

(6.3) If $t \in K^*$, then

$$\gamma'(t) = \gamma(t^{-1})\alpha(t^{3\theta-2})^{-1}h(\chi)\omega_0\alpha(-t^{3\theta-2})\gamma(t^{-1}),$$

where χ is defined by $\chi(a) = t^{2-4\theta}$, $\chi(b) = t^{6\theta-4}$.

Proof. We have

$$\gamma'(t) = x_{-(2a+b)}(t^{\theta})x_{-(3a+2b)}(t).$$

From (6.2) we have

$$x_{-(3a+2b)}(t) = x_{3a+2b}(t^{-1})h(\chi_1)\omega_{3a+2b}x_{3a+2b}(t^{-1}),$$

where

$$\chi_1 = \chi_{3a+2b,-t^{-1}}$$

On the other hand, we have by (1.6) and (1.10)

$$x_{-(2a+b)}(t^{\theta}) = \omega_a\omega_b x_{-a}(t^{\theta})\omega_{-b}\omega_{-a}.$$

Hence we have

$$\gamma'(t) = \omega_a\omega_b x_{-a}(t^{\theta})x_{3a+b}(t^{-1})\omega_{-b}\omega_{-a}h(\chi_1)\omega_{3a+2b}x_{3a+2b}(t^{-1}).$$

By transforming the first equation in (4.7) by ω_a, we obtain an expression of the form given in (1.2) for $(x_{-a}(t), x_{3a+b}(u))$. Combining this with (4.7), we get

$$\begin{aligned} & x_{-a}(t^{\theta})x_{3a+b}(t^{-1})x_{-a}(-t^{\theta}) \\ & \qquad = x_{3a+b}(t^{-1})x_{2a+b}(t^{\theta-1})x_{3a+2b}(-t^{3\theta-2})x_{a+b}(-t^{2\theta-1})x_b(t^{3\theta-1}). \end{aligned}$$

Hence we have from the above

$$\begin{aligned} \gamma'(t) &= \omega_a\omega_b x_{3a+b}(t^{-1})x_{2a+b}(t^{\theta-1})x_{3a+2b}(-t^{3\theta-2})x_{a+b}(-t^{2\theta-1}) \\ &\qquad \cdot x_b(t^{3\theta-1})x_{-a}(t^{\theta})\omega_{-b}\omega_{-a}h(\chi_1)\omega_{3a+2b}x_{3a+2b}(t^{-1}) \\ &= \omega_a x_{3a+2b}(t^{-1})x_{2a+b}(t^{\theta-1})x_{3a+b}(t^{3\theta-2})x_a(t^{2\theta-1})x_{-b}(-t^{3\theta-1}) \\ &\qquad \cdot x_{-(a+b)}(t^{\theta})\omega_{-a}h(\chi_1)\omega_{3a+2b}x_{3a+2b}(t^{-1}) \\ &= x_{3a+2b}(t^{-1})x_{a+b}(-t^{\theta-1})x_b(-t^{3\theta-2})x_{-a}(-t^{2\theta-1})x_{-(3a+b)}(-t^{3\theta-1}) \\ &\qquad \cdot x_{-(2a+b)}(t^{\theta})h(\chi_1)\omega_{3a+2b}x_{3a+2b}(t^{-1}). \end{aligned}$$

From (6.2) we have

$$x_{-a}(-t^{2\theta-1}) = x_a(-t^{1-2\theta})h(\chi_2)\omega_{-a}x_a(-t^{1-2\theta}),$$

where

$$\chi_2 = \chi_{a,-t^{1-2\theta}}.$$

Hence

$$\begin{aligned} \gamma'(t) &= x_{3a+2b}(t^{-1})x_{a+b}(-t^{\theta-1})x_b(-t^{3\theta-2})x_a(-t^{1-2\theta})h(\chi_2)\omega_{-a}x_a(-t^{1-2\theta}) \\ &\qquad \cdot x_{-(3a+b)}(-t^{3\theta-1})x_{-(2a+b)}(t^{\theta})h(\chi_1)\omega_{3a+2b}x_{3a+2b}(t^{-1}) \\ &= x_{3a+2b}(t^{-1})x_{a+b}(-t^{\theta-1})x_b(-t^{3\theta-2})x_a(-t^{1-2\theta})h(\chi_2)\omega_{-a}\omega_{3a+2b} \\ &\qquad \cdot x_a(-t^{1-2\theta})x_b(t^{3\theta-1})x_{a+b}(-t^{\theta})h(\chi_1 \circ w_{3a+2b})x_{3a+2b}(t^{-1}) \\ &= \gamma(t^{-1})\alpha(t^{3\theta-2})^{-1}h(\chi_2)h(\chi_1 \circ w_{3a+2b})^{-1}\omega_0 \\ &\qquad \cdot x_a(-t^{1-2\theta})x_b(-t^{3\theta-2})x_{a+b}(t^{\theta-1})x_{3a+2b}(t^{-1}), \end{aligned}$$

since $\omega_{-a}\omega_{3a+2b} = \omega_0$ by (3.8). Hence we have easily

$$\gamma'(t) = \gamma(t^{-1})\alpha(t^{3\theta-2})^{-1}h(\chi)\omega_0\alpha(-t^{3\theta-2})\gamma(t^{-1}),$$

where

$$\chi = \chi_2(\chi_1 \circ w_{3a+2b})^{-1},$$

from which it can be verified easily that $\chi(a) = t^{2-4\theta}$, $\chi(b) = t^{6\theta-4}$. Thus (6.3) is proved.

(6.4)[9] The element $h_0 = h(\chi)$, where $\chi(a) = \chi(b) = -1$, is contained in G^1. h_0 commutes with ω_0, and, for all $t \in K$,

$$h_0\alpha(t)h_0^{-1} = \alpha(-t), \quad h_0\beta(t)h_0^{-1} = \beta(t), \quad h_0\gamma(t)h_0^{-1} = \gamma(-t).$$

---

[9] The idea of deriving the proposition (6.4) from the canonical form of $\alpha'(t)$ is due to Tits. The author originally proved (6.4) under the assumption that K is finite, using (6.3) and (8.6).

Proof. The first part of (6.4) can be proved by setting $t=1$ in (6.1). The second part is a special case of $\omega_0 h \omega_0^{-1} = h^{-1}$, $h \in \mathfrak{H}$, which follows from (1.7). The third part follows from (5.12).

7. The simplicity of G^1. We shall prove the simplicity of G^1 under the assumption that the field K has more than 3 elements. If K has only 3 elements, then G^1, which is of order $2^3 \cdot 3^3 \cdot 7$, does not seem to be simple, although the author has been unable to verify this; also it is unlikely that any new simple group appears as a composition factor of G^1. In what follows, however, we shall arrange the proof of the simplicity of G^1 in such a way that we use the assumption on K only in the last stage.

Let $H \neq \{1\}$ be a normal subgroup of G^1. Denote, as in Section 5, by $\mathfrak{U}^1$, $\mathfrak{H}^1$, the groups of σ-invariant elements in $\mathfrak{U}$ and $\mathfrak{H}$, respectively.

(7.1) H contains an element $uh \neq 1$, where $u \in \mathfrak{U}^1$, $h \in \mathfrak{H}^1$.

Proof. By (5.16) we can assume that H contains $x = uh\omega_0$, where $u \in \mathfrak{U}^1$, $h \in \mathfrak{H}^1$. Let $h_0 \in G^1$ be the element defined in (6.4). Then $h_0 u h_0^{-1} u^{-1} u h \omega_0 \in H$, and hence $y = h_0 u h_0^{-1} u^{-1} \in H$. Since $y \in \mathfrak{U}^1$, we obtain (7.1) if $y \neq 1$. Hence we shall assume $y = 1$. Then from (6.4) and (5.5) we have $u = \beta(t_0)$ with some $t_0 \in K$. Hence $x = \beta(t_0) h \omega_0 \in H$. Let $h = h(\chi)$. Since, by (5.12),

$$\gamma(\chi(b)^{3\theta+2}t)\beta(t_0)h(\chi)\omega_0\gamma(\chi(b)^{3\theta+2}t)^{-1} = \beta(t_0)\gamma(\chi(b)^{3\theta+2}t)\gamma'(t)h(\chi)\omega_0,$$

and since $h(\chi)\omega_0\beta(t_0) \in H$, it folllows that H contains $x_1 = \gamma(\chi(b)^{3\theta+2}t)\gamma'(t)$ for all $t \in K$. By (6.1),

$$x_1 = \gamma(\chi(b)^{3\theta+2}t)\gamma(t^{-1})\alpha(t^{3\theta-2})^{-1}h(\chi_1)\omega_0\alpha(-t^{3\theta-2})\gamma(t^{-1}),$$

where χ_1 is defined by $\chi_1(a) = t^{2-4\theta}$, $\chi_1(b) = t^{6\theta-4}$. Hence H contains

$$\begin{aligned} x_2 &= \alpha(-t^{3\theta-2})\gamma(t^{-1})x_1\gamma(t^{-1})^{-1}\alpha(-t^{3\theta-2})^{-1}x^{-1} \\ &= \alpha(-t^{3\theta-2})\gamma(\chi(b)^{3\theta+2}t - t^{-1})\alpha(t^{3\theta-2})^{-1}h(\chi_1)h(\chi)^{-1}\beta(t_0)^{-1}. \end{aligned}$$

It is clear, in view of (5.6) and (5.12), that $x_2 \in \mathfrak{U}^1\mathfrak{H}^1$ and that $x_2 \neq 1$ if $t \neq 0$. Hence (7.1) is proved.

(7.2) H contains an element $\neq 1$ in $\mathfrak{U}^1$.

Proof. By (7.1), H contains $uh \neq 1$, $u \in \mathfrak{U}^1$, $h \in \mathfrak{H}^1$. Assume $h = h(\chi) \neq 1$. Then by (5.11) $\chi(b) \neq 1$. For any $t \in K$, H contains the element

$$\begin{aligned} uh\gamma(t)h^{-1}u^{-1}\gamma(t)^{-1} &= u\gamma(\chi(b)^{3\theta+2}t)u^{-1}\gamma(t)^{-1} \\ &= \gamma((\chi(b)^{3\theta+2}-1)t) \end{aligned}$$

which is $\neq 1$ if $t \neq 0$, since $\chi(b)^{3\theta+2} - 1 = 0$ would imply $\chi(b) = 1$ because of (5.1).

(7.3) H contains an element $\gamma(t)$, $t \neq 0$.

Proof. By (7.2), H contains an element $u \neq 1$ in $\mathfrak{U}^1$.

If $u = \alpha(t_1)\beta(t_2)\gamma(t_3)$ with $t_1 \neq 0$, then for any $t \in K$, H contains, by (5.6),

$$u^{-1}\beta(t)^{-1}u\beta(t) = u^{-1}\alpha(t_1)\beta(t_2)\gamma(t_3 + tt_1) = \gamma(tt_1).$$

If $u = \beta(t_2)\gamma(t_3)$ with $t_2 \neq 0$, then for any $t \in K$, H contains

$$u^{-1}\alpha(t)^{-1}u\alpha(t) = u^{-1}\beta(t_2)\gamma(t_3 - tt_2) = \gamma(-tt_2).$$

In any case, H contains an element $\gamma(t)$ with $t \neq 0$.

(7.4) If H contains $\gamma(t)$, $t \neq 0$, then H contains $\gamma(z^{3\theta+1}t)$ for all $z \in K^*$, and, in particular, $\gamma(t^{-1}) \in H$.

Proof. Let $h(\chi) \in \mathfrak{H}^2$ be such that $\chi(b) = z^{3\theta-1}$. Then $\chi(a) = \chi(b)^\theta = z^{1-\theta}$; $\chi(3a+2b) = z^{3\theta+1}$. By (5.13), H contains

$$h(\chi)\gamma(t)h(\chi)^{-1} = \gamma(\chi(3a+2b)t) = \gamma(z^{3\theta+1}t)$$

for any $z \in K^*$. Now set $z = t^{1-3\theta}$. Then $z^{3\theta+1} = t^{-2}$. Hence H contains $\gamma(t^{-1})$.

(7.5) If H contains $\gamma(t)$, $t \neq 0$, then H contains $\alpha(t^{3\theta-2})\beta(t^{1-3\theta})$ and $h(\chi)\omega_0$, where χ is defined by $\chi(a) = t^{2-4\theta}$, $\chi(b) = t^{6\theta-4}$.

Proof. Since G^1 contain ω_0 by (5.9), $\gamma(t) \in H$ implies that $\gamma'(t) \in H$. Then from (6.3) and (7.4) we can conclude that H contains $\alpha(-t^{3\theta-2})\alpha(t^{3\theta-2})^{-1}h(\chi)\omega_0$, where χ is defined by $\chi(a) = t^{2-4\theta}$, $\chi(b) = t^{6\theta-4}$. Since

$$\alpha(u)^{-1} = \alpha(-u)\beta(-u^{3\theta+1})\gamma(u^{3\theta+2})$$

by (5.6), H contains

$$\alpha(-t^{3\theta-2})\alpha(-t^{3\theta-2})\beta(-t^{1-3\theta})\gamma(t^{-1})h(\chi)\omega_0 = \alpha(t^{3\theta-2})\beta(t^{1-3\theta})\gamma(t^{-1})h(\chi)\omega_0.$$

Then by (7.4) H contains $x_1 = \alpha(t^{3\theta-2})\beta(t^{1-3\theta})h(\chi)\omega_0$. Replacing t by $-t$, we see that H also contains $x_2 = \alpha(-t^{3\theta-2})\beta(t^{1-3\theta})h(\chi)\omega_0$. Hence H contains

$$x_2x_1^{-1} = \alpha(-t^{3\theta-2})\alpha(t^{3\theta-2})^{-1} = \alpha(t^{3\theta-2})\beta(t^{1-3\theta})\gamma(t^{-1}).$$

Hence by (7.4) H contains $\alpha(t^{3\theta-2})\beta(t^{1-3\theta})$. Then H contains $h(\chi)\omega_0$, since $x_1 \in H$. Thus (7.5) is proved.

(7.6) H contains ω_0, $\gamma(t)$, $\alpha(t)\beta(t^{3\theta+1})$, and $h(\chi)$ for all $t \in K^*$, where χ is defined by $\chi(a) = t^{2\theta}$, $\chi(b) = t^2$.

Proof. By (7.3) and (7.5), H contains $x = \alpha(t_0^{3\theta-2})\beta(t_0^{1-3\theta})$ for some $t_0 \in K^*$. Hence H contains

$$\beta(u)x\beta(u)^{-1}x^{-1} = \gamma(-ut_0^{3\theta-2}).$$

Since u is an arbitrary element in K, it follows that H contains $\gamma(t)$ for all $t \in K$. Now we can set $t = 1$ in (7.5). Then $h(\chi) = 1$, and hence $\omega_0 \in H$. The rest of (7.6) follows immediately from (7.5) and the fact that $t^{3\theta-2}$ can be an arbitrary element in K^*.

(7.7) H contains the element h_0 defined in (6.4).

Proof. Since H contains ω_0 by (7.6), it follows that H contains

$$\alpha(-t)^{-1}\omega_0\alpha(-t)\omega_0^{-1} = \alpha(-t)^{-1}\alpha'(t);$$

which is, by (6.1), equal to

$$\alpha(-t)^{-1}\gamma(t^{-(3\theta+2)})\beta(t^{-(3\theta+1)})\alpha(t^{-1})^{-1}h(\chi)\omega_0\alpha(t^{-1})\beta(t^{-(3\theta+1)})\gamma(t^{-(3\theta+2)}),$$

where χ is defined by $\chi(a) = -t^{-2\theta}$, $\chi(b) = -t^{-2}$. Hence by (7.6) H contains

$$\alpha(-t)^{-1}\beta(t^{-(3\theta+1)})\alpha(t^{-1})^{-1}h_0.$$

Since H contains $\alpha(-t)^{-1}\beta(t^{3\theta+1})^{-1}$ and $\alpha(t^{-1})\beta(t^{-(3\theta+1)})$ by (7.6), we can conclude that H contains $\beta(t^{3\theta+1})\beta(-t^{-(3\theta+1)})h_0$ for any $t \in K^*$. Setting $t = 1$, we have $h_0 \in H$.

THEOREM 7.8. *If K contains more than 3 elements, then the group G^1 is simple.*

Proof. Let $H \neq \{1\}$ be a normal subgroup of G^1. By (7.6), H contains $h(\chi)$ where χ is defined by $\chi(a) = t^{2\theta}$, $\chi(b) = t^2$. Hence by (5.12), H contains

$$\beta(u)^{-1}h(\chi)\beta(u)h(\chi)^{-1} = \beta((t^{6\theta+2} - 1)u)$$

for every $t \neq 0$ and u in K. By (5.1) $t^{6\theta+2} - 1 = 0$ would imply $t^4 = 1$. Since K has more than 5 elements, there exists $t \in K^*$ such that $t^4 \neq 1$. Therefore H contains $\beta(t)$ for all $t \in K$. Then from (7.6) it follows that H contains ω_0, $\alpha(t)$, $\beta(t)$, and $\gamma(t)$ for all $t \in K$. Hence $H = G^1$. This proves the simplicity of G^1.

8. Further results on G^1. First we shall consider 2-subgroups of G^1.

(8.1) If $t \in K^*$, then

$$\beta'(t) = \beta(t^{-1}) h(\chi) \omega_0 \beta(t^{-1}),$$

where χ is defined by $\chi(a) = t^{\theta-1}$, $\chi(b) = t^{1-3\theta}$.

Proof. Applying ϕ_r to (6.2), we obtain

$$x_{-r}(t) = x_r(t^{-1}) h(\chi_{r,-t^{-1}}) \omega_r x_r(t^{-1}).$$

Since any one of $x_{a+b}(t)$, $x_{-(a+b)}(t)$ commute with any one of $x_{3a+b}(u)$, $x_{-(3a+b)}(u)$, and since $\omega_{a+b}\omega_{3a+b} = \omega_0$ by (3.8), we have from the above

$$\beta'(t) = x_{-(a+b)}(t^{\theta}) x_{-(3a+b)}(t) = \beta(t^{-1}) h(\chi) \omega_0 \beta(t^{-1}),$$

where

$$\chi = \chi_{a+b,-t^{-\theta}} \chi_{3a+b,-t^{-1}}.$$

It can be verified easily that $\chi(a) = t^{\theta-1}$, $\chi(b) = t^{1-3\theta}$. Thus (8.1) is proved.

(8.2) The element $x_0 = \beta(1)\omega_0\beta(-1)$ commutes with ω_0.

Proof. From (8.1) we have

$$\beta'(1) = \beta(1)\omega_0\beta(1), \qquad \beta'(-1) = \beta(-1)\omega_0\beta(-1).$$

Hence $x_0 = \beta'(1)\beta(1) = \beta(-1)\beta'(-1)$, from which it follows immediately that $\omega_0 x_0 \omega_0^{-1} = x_0$.

THEOREM 8.3. *The group G^1 contains an elementary abelian 2-subgroup of order* 8.

Proof. Let x_0 and h_0 be the elements defined in (8.2) and (6.4), respectively. Then, by (8.2) and (6.4), it is clear that the 3 elements x_0, h_0, ω_0 of order 2 commute with each other. By (5.16), h_0 and ω_0 generate a subgroup of order 4 which does not contain x_0. Hence x_0, h_0, and ω_0 generate an elementary abelian 2-group of order 8.

Now assume that K is a finite field of $q = 3^{2n+1}$ elements, where $n = 0, 1, 2, \cdots$. Then the automorphism θ of K defined by $t^{\theta} = t^{m}$, where $m = 3^{n}$, satifies $3\theta^2 = 1$. Hence the group G^1 can be defined. Since K^* is a cyclic group of order $q-1$, the subgroup K^{*2} of square elements is of index 2 in K^*. By (5.4), $-1 \notin K^2$. Hence K^* is generated by K^{*2} and -1. Hence by (6.1), (6.4), and (5.16) we have

(8.4) If K is finite, then G^1 is the group of all σ-invariant elements in G.

By (5.16) and (8.4), above, the order of G^1 is

$$q^3(q-1)+q^6(q-1)=q^3(q-1)(q^3+1).$$

Since $q-1\equiv 2 \pmod 8$, $q^3+1\equiv 4 \pmod 8$, the above order is divisible by 8 but not by 16. The 2-subgroup of order 8 given in (8.3) is then a Sylow subgroup. Hence

THEOREM 8.5. *If K is a finite field of $q=3^{2n+1}$ elements, where $n=0,1,2,\cdots$, then the order of G^1 is $q^3(q-1)(q^3+1)$, and a Sylow 2-subgroup of G^1 is an elementary abelian 2-group of order* 8.

All the previously known finite simple groups whose orders contain the prime 2 with the exact exponent 3 are: $L_3(2)$, $L_2(q)$ with $q\equiv\pm 7 \pmod{16}$, and the alternating group of degree 7 (cf. [1]). Among these only the first group, of order 168, has an elementary abelian Sylow 2-subgroup, and for the rest the Sylow 2-subgroups are dihedral. Hence Theorem 8.5, above, shows that the finite simple groups of the form G^1 are new. In passing, we note that all the known finite simple groups whose orders contain the prime 2 with the exact exponent 2 are the groups $L_2(q)$ with $q\equiv\pm 3 \pmod 8$, $q>3$ (cf. [1]). The Sylow 2-subgroups of these groups are, of course, elementary abelian, since they cannot be cyclic.

We shall devote the rest of this section to a study of the group S of all $z\in K^*$ such that $\chi(b)=z$ for some $h(\chi)\in G^1$. If K is finite, then (8.4) shows that $S=K^*$. In the general case, we already know that $z^{3\theta-1}\in S$ for any $z\in K^*$ by (5.13), and that $-1\in S$ by (6.4). Except for these, however, we know very little about S. We shall prove

THEOREM 8.6. *We have $1+z^2\in S$ for any $z\in K$.*

First we shall prove a few lemmas.

(8.7) Let

$$x=x_{3a+2b}(t_{32})x_{3a+b}(t_{31})x_{2a+b}(t_{21})x_{a+b}(t_{11})x_b(t_{01})x_a(t_{10})\omega_0$$

with $t_{ij}\in K$. If

$$t_{10}\neq 0,\ 1-t_{31}\neq 0,\ 1+t_{10}t_{21}-t_{31}\neq 0,$$

then

$$x_{-(3a+b)}(-1)x=x_{3a+2b}(u_{32})x_{3a+b}(u_{31})x_{2a+b}(u_{21})x_{a+b}(u_{11})$$
$$\cdot x_b(u_{01})x_a(u_{10})h(\chi)\omega_0x',$$

where $x'\in\mathfrak{U}$, where χ is defined by

$$\chi(a)=(1+t_{10}t_{21}-t_{31})^{-2}(1-t_{31}),$$
$$\chi(b)=(1+t_{10}t_{21}-t_{31})^{3}(1-t_{31})^{-2},$$

and where

$$\begin{aligned} u_{11} &= t_{11} + t_{10}^{-2}t_{31} - (t_{21} - t_{10}^{-1}t_{31})^2 \\ &\quad - (t_{10}^{-1}t_{31} - t_{21} - t_{10}^{-1})^2 t_{31}(1 - t_{31})^{-1}, \\ u_{10} &= -(t_{10}^{-1}t_{31} - t_{21} - t_{10}^{-1})^{-1}, \\ u_{01} &= t_{32} - t_{10}^{-3}t_{31}^2 - t_{01}t_{31} + t_{01} - t_{10}^{-3}t_{31} \\ &\quad + (t_{21} - t_{10}^{-1}t_{31})^3 - (t_{10}^{-1}t_{31} - t_{21} - t_{10}^{-1})^3 t_{31}(1 - t_{31})^{-1}. \\ u_{32} &= t_{32} - t_{10}^{-3}t_{31}^2 - t_{01}t_{31} - (t_{21} - t_{10}^{-1}t_{31})^3 \\ &\quad - (t_{10}^{-1}t_{31} - t_{21} - t_{10}^{-1})^3 t_{31}^2(1 - t_{31})^{-2}. \end{aligned}$$

Proof. We merely follow the steps (1.15)-(1.17) mechanically to find the canonical form of the element $x_{-(3a+b)}(-1)x = \omega_a x_{-b}(-1)\omega_a^{-1}x$. We omit the details.

(8.8) Let

$$y = x_{3a+2b}(u_{32})x_{3a+b}(u_{31})x_{2a+b}(u_{21})x_{a+b}(u_{11})x_b(u_{01})x_a(u_{10})\omega_0$$

with $u_{ij} \in K$. If

$$u_{01} \neq 0, 1 - u_{11} - u_{01}u_{10} \neq 0, 1 + u_{01}u_{32} - u_{11}^3 \neq 0,$$

then we have

$$x_{-(a+b)}(-1)y = y''h(\chi_1)\omega_0 y',$$

where y' and y'' are in $\mathfrak{U}$, and where χ_1 is given by

$$\begin{aligned} \chi_1(a) &= (1 + u_{01}u_{32} - u_{11}^3)(1 - u_{11} - u_{01}u_{10})^{-2}, \\ \chi_1(b) &= (1 + u_{01}u_{32} - u_{11}^3)^{-2}(1 - u_{11} - u_{01}u_{10})^3. \end{aligned}$$

Proof. We make use of the automorphism σ of G. Set

$$x = y^\sigma = x_{3a+2b}(t_{32})x_{3a+b}(t_{31}) \cdots x_a(t_{10})\omega_0.$$

Then by an easy computation we get

$$t_{10} = u_{01}^\theta, \quad t_{31} = u_{11}^{3\theta} + u_{01}^{3\theta}u_{10}^{3\theta}, \quad t_{21} = u_{32}^\theta + u_{01}^{2\theta}u_{10}^{3\theta}.$$

Hence $t_{10} \neq 0$, $1 - t_{31} \neq 0$ are clear. Also

$$t_{31} - t_{10}t_{21} = u_{11}^{3\theta} - u_{01}^\theta u_{32}^\theta = (u_{11}^3 - u_{01}u_{32})^\theta \neq 1.$$

Hence we can apply (8.7) to x. Set

$$x_{-(3a+b)}(-1)x = x''h(\chi)\omega_0 x',$$

where x', x'' are in $\mathfrak{U}$ and where χ is given in (8.7). Applying σ to the above, we get

$$x_{-(a+b)}(-1)y = y''h(\bar{\chi})\omega_0 y',$$

where $y'' = (x'')^\sigma$, $y' = (x')^\sigma$. Hence we can set $\chi_1 = \chi$. We shall compute the values of χ_1. By (8.7) we have

$$\begin{aligned}\chi(a) &= (1 + t_{10}t_{21} - t_{31})^{-2}(1 - t_{31}) \\ &= (1 + u_{01}{}^{\theta}u_{32}{}^{\theta} - u_{11}{}^{3\theta})^{-2}(1 - u_{11}{}^{3\theta} - u_{01}{}^{3\theta}u_{10}{}^{3\theta}).\end{aligned}$$

Since $\chi_1(b) = \chi(a)^{3\theta}$ by (5.10), we have

$$\chi_1(b) = (1 + u_{01}u_{32} - u_{11}{}^{3})^{-2}(1 - u_{11} - u_{01}u_{10})^{3}.$$

Similarly we can compute $\chi_1(a)$. Thus (8.8) is proved.

Proof of Theorem 8.6. Set $x = \gamma(-t^{3\theta+2})\alpha(-t)^{-1}\omega_0$ with $t \neq 0, \pm 1$. Then

$$x = x_{3a+2b}(-t^{3\theta+2})x_{a+b}(-t^{\theta+1})x_b(t)x_a(t^\theta)\omega_0$$

Since $t \neq 0$, we can apply (8.7) to x. We obtain

$$y = x_{-(3a+b)}(-1)x = x_{3a+2b}(u_{32}) \cdots x_b(u_{01})x_a(u_{10})\omega_0 x',$$

where $x' \in \mathfrak{U}$, and

$$u_{11} = -t^{\theta+1}, \quad u_{01} = -t^{3\theta+2} + t, \quad u_{32} = -t^{3\theta+2}, \quad l_{01} = t^\theta.$$

We wish to apply (8.8) to y. The condition on u_{ij} in (8.8) are easily found to be equivalent to $t^2 \neq \pm 1$, and hence by (5.4), to $t \neq \pm 1$. Since these are assumed, we can apply (8.8) to y, and obtain

$$\beta'(-1)x = x_{-(a+b)}(-1)y = y''h(\chi_1)\omega_0 y',$$

where y', y'' are in $\mathfrak{U}^1$ (since x and $\beta'(-1)$ are σ-invariant), and where $h(\chi_1)$, which is also σ-invariant, is given by

$$\chi_1(b) = (1 + t^{6\theta+4})^{-2}(1 + t^{4\theta+2})^{3}.$$

Since x is in G^1, it is clear from the above that $h(\chi_1)$ is in G^1. By (6.1) and (6.4), $K^{*2} \subseteq S$. Then the above implies that $1 + t^{4\theta+3} \in S$ whenever $t \neq 0, \pm 1$. Write $z = t^{2\theta+1}$. Then $t = z^{6\theta-3}$, and the conditions $t \neq 0, \pm 1$ are easily seen to be equivalent to $z \neq 0, \pm 1$. If $z = 0$ or ± 1, then $1 + z^3 = \pm 1$, and hence by (6.4) $1 + z^2 \in S$. Thus (8.6) is proved.

9. Automorphisms of G^1. If $t \rightarrow t'$ is an automorphism of the field K which commutes with θ, then, since G^1 is generated by $\alpha(t), \cdots, \gamma'(t)$, it can be seen easily that the map $\alpha(t) \rightarrow \alpha(t'), \cdots, \gamma'(t) \rightarrow \gamma'(t')$ can be extended to an automorphism ρ of G^1. We shall call ρ the automorphism of G^1 induced by the automorphism $t \rightarrow t'$ of K. If K is a finite field, then any automorphism of K commutes with θ and hence induces an automorphism of G^1. We shall prove

THEOREM 9.1. *If K is a finite*[10] *field possessing more than 3 elements, then every automorphism of G^1 can be written uniquely in the form $\rho_1\rho_2$, were ρ_1 is an automorphism of G^1 induced by an automorphism of K and where ρ_2 is an inner automorphism of G^1.*

Proof. Let $x \rightarrow x^\rho$ be an automorphism of G^1. Since $\mathfrak{U}^1$ is clearly a Sylow 3-subgroup of G^1, and since any two Sylow 3-subgroups are conjugate, it follows that $\mathfrak{U}^1$ and $(\mathfrak{U}^1)^\rho$ are conjugate; there exists an inner automorphism ρ' such that $\rho\rho'$ maps $\mathfrak{U}^1$ onto itself. Hence we can assume from the beginning that

$$(9.2) \qquad (\mathfrak{U}^1)^\rho = \mathfrak{U}^1.$$

By (5.6) it can be seen easily that the center of $\mathfrak{U}^1$ consists of the elements $\gamma(t)$, $t \in K$. Hence by (9.2) there exists an automorphism $t \rightarrow t'$ of the additive group of K such that $\gamma(t)^\rho = \gamma(t')$. Write $c = 1' \neq 0$. Since K is assumed to be finite, there exists, by (8.4), $h = h(\chi) \in G^1$ such that $\chi(b) = c^{3\theta-2}$. Denote by ρ' the inner automorphism defined by $x^{\rho'} = hxh^{-1}$. Then $\gamma(t)^{\rho\rho'} = h\gamma(t')h^{-1} = \gamma(\chi(b)^{3\theta+2}t') = \gamma(c^{-1}t')$, and hence $\gamma(1)^{\rho\rho'} = \gamma(1)$. Clearly ρ' maps $\mathfrak{U}^1$ onto itself. Hence we can assume from the beginning that ρ satisfies not only (9.2) but also

$$(9.3) \qquad \gamma(t)^\rho = \gamma(t'),$$

where $t \rightarrow t'$ is an automorphism of the additive group of K such that $1' = 1$.

We shall show that the group $\mathfrak{U}^1\mathfrak{H}^1$ is the normalizer of $\mathfrak{U}^1$ in G^1. It is clear that $\mathfrak{U}^1\mathfrak{H}^1$ normalizes $\mathfrak{U}^1$. Suppose $x \in G^1$ normalizes $\mathfrak{U}^1$, and let $x = uh\omega u_1$ be the canonical form of x given in (5.16). Then ω normalizes $\mathfrak{U}^1$. Hence $\omega \neq \omega_0$, and we have $\omega = 1$. Thus $x \in \mathfrak{U}^1\mathfrak{H}^1$. Then by (9.2) we get

$$(9.4) \qquad (\mathfrak{U}^1\mathfrak{H}^1)^\rho = \mathfrak{U}^1\mathfrak{H}^1,$$

from which it follows that there exists a homomorphism $h(\chi) \rightarrow h(\chi')$ of H^1 into itself such that

$$(9.5) \qquad h(\chi)^\rho h(\chi')^{-1} \in \mathfrak{U}^1.$$

By (9.3) and (9.5) we obtain

$$\chi'(b)^{3\theta+2}t' = (\chi(b)^{3\theta+2}t)'.$$

---

[10] See footnote 3.

Setting $t=1$ in the above, and using $1'=1$ we obtain

$$\chi'(b)^{3\theta+2}=(\chi(b)^{3\theta+2})'. \tag{9.6}$$

Then from the above we get

$$(\chi(b)^{3\theta+2})'t'=(\chi(b)^{3\theta+2}t)'.$$

Since, by (8.4) and (5.3), every element in K^* can be written in the form $\chi(b)^{3\theta+2}$ with $h(\chi)\in G^1$, it follows that $u't'=(ut)'$ for any u, t in K. Since $t\to t'$ is an automorphism of the additive group of K, we have thus shown that the map $t\to t'$ is an automorphism of K. Denote by ρ' the automorphism of G^1 induced by the inverse of the automorphism $t\to t'$. Then $\gamma(t')^{\rho'\rho}=\gamma(t)^{\rho}=\gamma(t')$ for all $t\in K$. Also, it is clear that ρ' maps $\mathfrak{U}^1$ into itself. Hence we can assume, for the proof of Thseorem 9.1, that $t'=t$ for all $t\in K$. Then

$$\gamma(t)^{\rho}=\gamma(t) \tag{9.7}$$

for all $t\in K$, and, by (9.6), $\chi'=\chi$. Hence, by (9.5),

$$h(\chi)^{\rho}h(\chi)^{-1}\in\mathfrak{U}^1. \tag{9.8}$$

Now, by (5.16) one can show easily that $\omega_0\mathfrak{U}^1\omega_0^{-1}\cap\mathfrak{H}^1=\{1\}$, which, combined with (9.4), shows that ω_0^{ρ} must be of the form $\omega_0^{\rho}=uh\omega_0u'$, where u, $u'\in\mathfrak{U}^1$, $h\in\mathfrak{H}^1$. Then $\omega_0^2=1$ implies $uh\omega_0u'uh\omega_0u'=1$, which in turn implies $u'u=1$. Denote by ρ' the inner automorphism $x\to u^{-1}xu$ of G^1. Then $\omega_0^{\rho\rho'}=h\omega_0$, and we can replace ρ by $\rho\rho'$ in (9.2), (9.7), and (9.8) without losing the validity of the statements. Hence we can assume

$$\omega_0^{\rho}=h(\chi_0)\omega_0. \tag{9.9}$$

We shall show that $\rho=1$ follows from (9.2), (9.7), (9.8), and (9.9). This is clearly sufficient for the proof of Theorem 9.1. By (9.8) we can write $h(\chi)^{\rho}=u_{\chi}h(\chi)$ with $u_{\chi}\in\mathfrak{U}^1$. Substituting this and (9.9) to $\omega_0^{-1}h(\chi)\omega_0=h(\chi)^{-1}$ one can derive easily $u_{\chi}=1$. Thus we have, for all $h(\chi)\in\mathfrak{H}^1$,

$$h(\chi)^{\rho}=h(\chi). \tag{9.10}$$

By (9.2) we can write $\alpha(1)^{\rho}=\alpha(c)\beta(c_1)\gamma(c_2)$ with c, c_1, and c_2 in K. Then by (9.10), (5.12), and the fact that $\chi(b)$ can be regarded as an arbitrary element in K^*, we have

$$\alpha(t)^{\rho}=\alpha(ct)\beta(c_1t^{3\theta+1})\gamma(c_2t^{3\theta+2}) \tag{9.11}$$

for all $t\in K$.

Let $\mathfrak{Z}^1$ be the center of $\mathfrak{U}^1$, and $\mathfrak{Z}^2/\mathfrak{Z}^1$ the center of $\mathfrak{U}^1/\mathfrak{Z}^1$. Then by (5.6) one can see easily that $\mathfrak{Z}^2$ consists of the elements $\beta(t)\gamma(u), t, u \in K$. Hence $\beta(t)^\rho = \beta(t_1)\gamma(t_2)$. Let h_0 be the element defined in (6.4). Then by (9.10), $h_0^\rho = h_0$. Hence we have $\beta(t)^\rho = \beta(t_1)\gamma(-t_2)$. Then $t_2 = -t_2$, $t_2 = 0$. Thus we have $\beta(t)^\rho = \beta(t_1)$. Combining this and (9.11) with the second identity of (5.6) one can deduce easily $cut_1 = ut$ for all u, t in K. Hence $c \neq 0$, and $t_1 = c^{-1}t$. Thus we have proved that

$$\beta(t)^\rho = \beta(c^{-1}t) \tag{9.12}$$

holds for all $t \in K$. Now combining (9.11) and (9.12) with the first identity of (5.6) one can deduce

$$c_1(t+u)^{3\theta+1} - c^{-1}tu^{3\theta} = c_1t^{3\theta+1} + c_1u^{3\theta+1} - ct(cu)^{3\theta}$$

for all $t, u \in K$. Since

$$(t+u)^{3\theta+1} = t^{3\theta+1} + t^{3\theta}u + tu^{3\theta} + u^{3\theta+1}$$

we have $c_1t^{3\theta}u = (c^{-1} - c^{3\theta+1} - c_1)tu^{3\theta}$ for all $t, u \in K$. Now assume that K has more than 3 elements. Then we have $c_1 = 0$, $c^{-1} - c^{3\theta+1} - c_1 = 0$. Hence $c^{3\theta+2} = 1$, $c = 1$. Thus we have

$$\alpha(t)^\rho = \alpha(t)\gamma(c_2t^{3\theta+2}), \qquad \beta(t)^\rho = \beta(t)$$

for all $t \in K$. Combining these again with the first identity of (5.6), we can deduce

$$c_2(t+u)^{3\theta+2} = c_2t^{3\theta+2} + c_2u^{3\theta+2}$$

for all $t, u \in K$. Since

$$(t+u)^{3\theta+2} = t^{3\theta+2} + u^{3\theta+2} - t^{3\theta}(tu - u^2) + u^{3\theta}(t^2 - tu)$$

we have, by setting $u = 1$, $c_2(t^{3\theta} - t)(t-1) = 0$ for all $t \in K$. It can be easily seen that $t^{3\theta} - t = 0$ implies that $t = 0$ or ± 1. Since K is assumed to have more than 3 elements, we conclude $c_2 = 0$. Thus we have proved, for all $t \in K$,

$$\alpha(t)^\rho = \alpha(t), \qquad \beta(t)^\rho = \beta(t). \tag{9.13}$$

Now, by (8.1), (9.7), (9.9), (9.10), and (9.13), we have

$$h(\chi_0)\omega_0\beta(-1)\omega_0^{-1}h(\chi_0)^{-1} = \beta(1)h(\chi_0)\omega_0\beta(1).$$

Then by (5.12) we have

$$\beta'(\chi_0(b)^{-3\theta-1}) = \beta(1)h(\chi_0)\beta(1)^{-1}\beta'(1).$$

Then $\omega_0\mathfrak{U}^1\omega_0^{-1}\cap\mathfrak{U}^1=\{1\}$ implies $\beta(1)h(\chi_0)\beta(1)^{-1}=1$, $h(\chi_0)=1$. Thus we have proved $\omega_0^{\rho}=\omega_0$. Then by (9.7) and (9.13) we have $\rho=1$, since G^1 is generated by the elements $\alpha(t)$, $\beta(t)$, $\gamma(t)$, and ω_0. Thus the proof of Theorem 9.1 is complete, except for the uniqueness part.

To prove the uniqueness, let $t\to t'$ be an automorphism of K, and suppose that the automorphism of G^1 induced by it is the inner automorphism $x\to axa^{-1}$. Then clearly $a\mathfrak{U}^1a^{-1}=\mathfrak{U}^1$, and, since the normalizer of $\mathfrak{U}^1$ on G^1 is $\mathfrak{U}^1\mathfrak{H}^1$, a must be of the form $a=uh$, where $u\in\mathfrak{U}^1$, $h\in\mathfrak{H}^1$. On the other hand, since $1'=1$, $(-1)'=-1$, a must commute with $\omega_0=\beta(1)\beta'(-1)\beta(1)$. From this we can conclude easily $u=1$, $h=1$, and that $t\to t'$ is the identity automorphism of K. Thus the uniqueness part is also proved.

UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, B. C.

REFERENCES.

[1] E. Artin, "The orders of the classical simple groups," *Communications on Pure and Applied Mathematics*, vol. 8 (1955), pp. 455-472.

[2] C. Chevalley, "Sur certains groupes simples," *Tôhoku Mathematical Journal* (2), vol. 7 (1955), pp. 14-66.

[3] R. Ree, "On some simple groups defined by C. Chevalley," *Transactions of the American Mathematical Society*, vol. 84 (1957), pp. 392-400.

[4] R. Steinberg, "Variation on a theme of Chevalley," *Pacific Journal of Mathematics*, vol. 9 (1959), pp. 875-891.

[5] M. Suzuki, "A new type of simple groups of finite order," *Proceedings of the National Academy of Sciences*, vol. 46 (1960), pp. 868-870.

[6] J. Tits, "Sur les analogues algébriques des groupes semi-simples complexes," *Colloque d'algèbre supérieure*, Bruxelles, 1956, pp. 261-289.

[7] ———, "Les groupes simples de Suzuki et de Ree," *Séminaire Bourbaki*, December, 1960.

[8] R. Steinberg, "Automorphisms of finite linear groups," *Canadian Journal of Mathematics*, vol. 12 (1960), pp. 606-615.

[9] R. Ree, "A family of simple groups associated with the simple Lie algebra of type (F_4)," *American Journal of Mathematics*, vol. 83 (1961), pp. 401-420.

ALGEBRAIC ISOMORPHISMS BETWEEN ORDERED BASES.*

By J. R. Ringrose.

---

1. **Introduction.** Let H be a complex Hilbert space, and denote by (H, H) the class of all bounded linear operators acting in H. An *operator algebra over* H is a subset $\mathfrak{J}$ of (H, H) such that, if $A, B \in \mathfrak{J}$ and λ is a complex number, then $A + B, AB, \lambda A \in \mathfrak{J}$. If $\mathfrak{J}_1$, $\mathfrak{J}_2$ are operator algebras over Hilbert spaces H_1, H_2 respectively, an *algebraic isomorphism* from $\mathfrak{J}_1$ onto $\mathfrak{J}_2$ is a one to one linear and multiplicative mapping ϕ from $\mathfrak{J}_1$ onto $\mathfrak{J}_2$. If there is a non-singular continuous linear transformation Q from H_2 onto H_1 such that

$$\phi(T) = Q^{-1}TQ \qquad (T \in \mathfrak{J}_1),$$

we say that ϕ is a *spatial isomorphism*, and is *implemented by* Q. The main object of the present paper is to prove that, if $\mathfrak{J}_1$ and $\mathfrak{J}_2$ are ordered bases (in the sense of [3]), then every algebraic isomorphism from $\mathfrak{J}_1$ onto $\mathfrak{J}_2$ is spatial.

2. **Notation and definitions.** Let $\mathfrak{J}$ be an operator algebra over a Hilbert space H. We denote by $\mathfrak{J}^*$ the algebra $\{T^* : T \in \mathfrak{J}\}$. By a *hull* of $\mathfrak{J}$ we shall mean a closed subspace L of H which is invariant under each operator in $\mathfrak{J}$. A *hull idempotent* of $\mathfrak{J}$ is an idempotent in (H, H) whose range is a hull of $\mathfrak{J}$. A self-adjoint hull idempotent will be called a *hull projection*. *A full class of hull idempotents of* $\mathfrak{J}$ is a family $\mathfrak{F}$ of hull idempotents such that, given any hull L of $\mathfrak{J}$, there is a member of $\mathfrak{F}$ whose range is L.

Following Kadison and Singer [3], we shall say that the operator algebra algebra $\mathfrak{J}$ is a *maximal triangular algebra* if

(i) $\mathfrak{A} = \mathfrak{J} \cap \mathfrak{J}^*$ is a maximal abelian sub-algebra of (H, H);

(ii) amongst algebras satisfying (i), $\mathfrak{J}$ is maximal.

Under these conditions, $\mathfrak{A}$ is a commutative von Neumann algebra, called the *diagonal* of $\mathfrak{J}$. It is shown in [3] that the hulls of a maximal triangular algebra are linearly ordered (by inclusion), and that each hull projection lies

---

* Received December 6, 1960.

in the diagonal of the algebra. If the hull projections of a maximal triangular algebra $\mathfrak{J}$ generate the diagonal (as a von Neumann algebra), we shall call $\mathfrak{J}$ an *ordered basis*. The motivation for these definitions is indicated in [3]. We note that, owing to the need in this paper to consider non-orthogonal projections, our use of the term *hull* differs slightly from that of [3].

We now give an example which is of some importance in the theory. Let ρ be a non-negative measure defined on the Borel subsets of the closed interval $[0,1]$, and denote by H_ρ the space $L^2([0,1]:\rho)$ of ρ-measurable functions whose squares are ρ-summable over $[0,1]$. Given a ρ-essentially bounded function $f(t)$, let M_f be the operator of multiplication by f. The set

$$\mathfrak{A}_\rho = \{M_f : f \in L^\infty([0,1]:\rho)\}$$

is a maximal abelian sub-algebra of (H_ρ, H_ρ), the *multiplication algebra* over H_ρ. This algebra contains the orthogonal projection $E(\tau)$ of multiplication by the characteristic function of τ, whenever τ is a Borel subset of $[0,1]$. We refer to $E(\tau)$ as the *spectral measure in* $\mathfrak{A}_\rho$. We define $E_\lambda = E([0,\lambda])$, $E_{\lambda-} = E([0,\lambda))$ $(0 \leqq \lambda \leqq 1)$. Now let $\mathfrak{J}_\rho$ be the class of all bounded linear operators acting in H_ρ which leave invariant the range of each E_λ. Then $\mathfrak{J}_\rho$ is an ordered basis over H_ρ, with diagonal $\mathfrak{A}_\rho$ and hull projections E_λ, $E_{\lambda-}$ $(0 \leqq \lambda \leqq 1)$. For these facts we refer to [3]. The importance of this example lies in the following representation theorem, which is proved in [3] (see p. 248).

THEOREM. *Let $\mathfrak{J}$ be an ordered basis over a separable Hilbert space H. Then it is possible to choose a non-negative measure ρ defined on the Borel subsets of the interval $[0,1]$, and a unitary operator U from H onto H_ρ, in such a way that $\mathfrak{J} = U^{-1}\mathfrak{J}_\rho U$.*

As an immediate consequence of this theorem, we note that an ordered basis consists exactly of those operators which leave invariant each of its hulls.

If $\mathfrak{J}$ is an operator algebra over a Hilbert space H, we denote by $\mathfrak{J}'$ the commutant of $\mathfrak{J}$: that is,

$$\mathfrak{J}' = \{S \in (H,H) : ST = TS \ (T \in \mathfrak{J})\}.$$

The von Neumann algebras over H can be defined as those for which $\mathfrak{J} = \mathfrak{J}^* = (\mathfrak{J}')'$.

3. Some preliminary lemmas.

LEMMA 1. *The following properties of elements of an operator algebra*

$\mathcal{T}$ over a Hilbert space H are conserved by any algebraic isomorphism between two operator algebras.

(i) *E is idempotent.*

(ii) *E, E' are idempotents and $E(H) \subset E'(H)$.*

(iii) *E, E' are idempotents and $E(H) = E'(H)$.*

(iv) *E is a hull idempotent of $\mathcal{T}$.*

Proof. In order to prove parts (i), (ii) and (iv) we shall state in each case an equivalent property which is obviously preserved by algebraic isomorphism. Part (iii) is immediate from (ii).

(i) $E^2 = E$.

(ii) $E^2 = E'E = E$, $(E')^2 = E'$.

(iv) $E^2 = E$, $TE = ETE$ $(T \in \mathcal{T})$.

LEMMA 2. *Let $\mathcal{T}_1$, $\mathcal{T}_2$ be maximal triangular algebras, and let ϕ be an algebraic isomorphism from $\mathcal{T}_1$ onto $\mathcal{T}_2$. Then if $\mathcal{F}$ $(\subset \mathcal{T}_1)$ is a full set of hull idempotents for $\mathcal{T}_1$, the family $\phi(\mathcal{F}) = \{\phi(E) : E \in \mathcal{F}\}$ is a full set of hull idempotents for $\mathcal{T}_2$.*

Proof. It is immediate from Lemma 1(iv) that $\phi(\mathcal{F})$ is a family of hull idempotents for $\mathcal{T}_2$. Suppose now that L is any hull of $\mathcal{T}_2$, and let F be the corresponding hull projection. Since $\mathcal{T}_2$ is a maximal triangular algebra, $F \in \mathcal{T}_2$. Thus we may set $F = \phi(E)$, where $E \in \mathcal{T}_1$ and (by Lemma 1(iv)) is a hull idempotent of $\mathcal{T}_1$. Since $\mathcal{F}$ is a full set of hull idempotents for $\mathcal{T}_1$, there is an element E' in $\mathcal{F}$ having the same range as E. Let $\phi(E') = F'$. Then $F' \in \phi(\mathcal{F})$, and has the same range as F (by Lemma 1(iii)). Since the range of F is L, it follows that $\phi(\mathcal{F})$ is a full set of hull idempotents for $\mathcal{T}_2$.

LEMMA 3. *Let e, f be elements of the Hilbert space H_ρ, and let S be the bounded linear operator acting in H_ρ which is defined by the equation $Sx = \langle x, e\rangle f$ $(x \in H_\rho)$. Then a necessary and sufficient condition that S should be a member of the ordered basis $\mathcal{T}_\rho$ is that there exist a $\mu \in [0,1]$ such that $E_{\mu-}e = 0$, $E_\mu f = f$. The notations are those introduced in* § 2.

Proof. Suppose that $S \in \mathcal{T}_\rho$, and let $\mu = \inf\{\lambda : E_\lambda f = f\}$. The right continuity of E_λ implies that $E_\mu f = f$, while from the definition of μ it follows that $E_\lambda f \neq f$ $(\lambda < \mu)$. Now

$$SE_\lambda e = \| E_\lambda e \|^2 f,$$
$$E_\lambda SE_\lambda e = \| E_\lambda e \|^2 E_\lambda f.$$

Since $SE_\lambda = E_\lambda SE_\lambda$, while $f \neq E_\lambda f$ when $\lambda < \mu$, we deduce that for such λ, $E_\lambda e = 0$. When $\lambda \nearrow \mu$ we obtain $E_{\mu-}e = 0$.

Now suppose conversely that for some $\mu \in [0,1]$ we have $E_{\mu-}e = 0$, $E_\mu f = f$. If $\lambda < \mu$, then

$$SE_\lambda x = \langle E_\lambda x, e\rangle f = \langle x, E_\lambda e\rangle f = 0 \qquad (x \in H_\rho),$$

and thus $SE_\lambda = E_\lambda SE_\lambda$ $(\lambda < \mu)$. On the other hand, the last equation is satisfied when $\lambda \geqq \mu$, since then $f = E_\lambda f$. Hence S leaves invariant the range of each E_λ, and is therefore a member of $\mathfrak{J}_\rho$. This completes the proof of the lemma.

LEMMA 4. *Let $\mathfrak{J}$ be an ordered basis over a separable Hilbert space H, and suppose that $A \in \mathfrak{J}$. Then A has rank unity if and only if* (i) *$A \neq 0$, and* (ii) *if $B, C \in \mathfrak{J}$ and $BAC = 0$, then at least one of BA, AC is zero. Consequently, the property of having rank unity is preserved by algebraic isomorphism between ordered bases.*

Proof. We first suppose that A has rank unity. Then we may choose e, f $(\in H)$ in such a way that $Ax = \langle x, e\rangle f$ $(x \in H)$. We then have

$$BAx = \langle x, e\rangle Bf, \quad ACx = \langle x, C^*e\rangle f, \quad BACx = \langle x, C^*e\rangle Bf \qquad (x \in H).$$

If $BAC = 0$, one at least of C^*e, Bf is zero; hence one at least of BA, AC is zero. Since $A \neq 0$, conditions (i) and (ii) are satisfied.

Now suppose that A has rank exceeding unity. Because of the representation theorem for ordered bases which is stated in § 2, it is sufficient to consider the case in which $\mathfrak{J} = \mathfrak{J}_\rho$. We shall use the notations introduced in § 2, and write L_λ for the range of the projection E_λ. Let

$$\alpha = \sup\{\lambda : E_\lambda = 0\}, \qquad \beta = \inf\{\lambda : E_\lambda = I\}.$$

Thus $E_{\alpha-} = 0$, $E_\beta = I$. We now consider separately four possibilities, enumerated below as cases 1 and 2, in each of which there are alternatives (a) and (b).

Case 1. $\dim\{A(L_\lambda)\} > 1$ *for some* $\lambda < \beta$.

In this case let u_1, u_2 $(\in L_\lambda)$ be chosen in such a way that Au_1, Au_2 are linearly independent, and let $e(\neq 0) \in H_\rho \ominus L_\lambda$. We now sub-divide case 1 into two alternatives.

Alternative (a). *For some $\mu > \alpha$, $(I - E_\mu)Au_1$, $(I - E_\mu)Au_2$ are linearly independent.* Let $f(\neq 0) \in L_\mu$. We may assume (by making a non-singular transformation on u_1, u_2) that $(I-E_\mu)Au_1$, $(I-E_\mu)Au_2$ are orthogonal. We then define

$$Cx=\langle x,e\rangle u_1,\qquad Bx=\langle x,(I-E_\mu)Au_2\rangle f\qquad\qquad (x\in H_\rho).$$

It is easily verified by means of Lemma 3 that $B,C\in\mathfrak{J}_\rho$; furthermore, $BAC=0$. However, neither BA nor AC is zero, since $ACe\neq 0\neq BAu_2$.

Alternative (b). *For every* $\mu>\alpha$, $(I-E_\mu)Au_1$, $(I-E_\mu)Au_2$ *are linearly dependent.* We may choose scalars l_μ, m_μ $(\mu>\alpha)$ such that

$$|l_\mu|+|m_\mu|=1,\qquad l_\mu(I-E_\mu)Au_1+m_\mu(I-E_\mu)Au_2=0.$$

As $\mu\searrow\alpha$ through a suitable sequence, l_μ and m_μ tend to limits l, m (respectively), and we have

$$|l|+|m|=1,\qquad l(I-E_\alpha)Au_1+m(I-E_\alpha)Au_2=0.$$

It follows that $(I-E_\alpha)Au_1$, $(I-E_\alpha)Au_2$ are linearly dependent, and hence that $E_\alpha\neq 0$. If we now set $u_0=lu_1+mu_2$, then $0\neq Au_0=E_\alpha Au_0$. Since $E_\alpha=E_\alpha-E_{\alpha-}$, we may describe E_α as the projection of multiplication by the function taking the value unity at α and vanishing elsewhere. Thus the single point α has positive ρ-measure, and E_α is an operator of rank unity. Since $\dim\{A(L_\lambda)\}>1$, we may choose u_3 $(\in L_\lambda)$ such that $E_\alpha Au_3=0\neq Au_3$. If we now define $B=E_\alpha$, $Cx=\langle x,e\rangle u_3$ $(x\in H_\rho)$, then it is easily verified that $B,C\in\mathfrak{J}_\rho$. Furthermore, $BAC=0$, but $ACe\neq 0\neq BAu_0$.

Case 2. $\sup\limits_{\lambda<\beta}\dim\{A(L_\lambda)\}=r\leqq 1.$

In this case we have $\dim\{A(L_\mu)\}=r$ for some $\mu<\beta$. Then $A(L_\lambda)=A(L_\mu)$ $(\mu\leqq\lambda<\beta)$, and hence $A(L_{\beta-})=A(L_\mu)$ (where $L_{\beta-}$ is the range of the projection $E_{\beta-}$). We deduce that $\dim\{A(L_{\beta-})\}=r\leqq 1$, and thus that $L_{\beta-}\neq H_\rho=L_\beta$. It follows that $L_{\beta-}$ has codimension unity in H_ρ. Let $e(\neq 0)\in H_\rho\ominus L_{\beta-}$. Since H_ρ is spanned by e and $L_{\beta-}$, $A(H_\rho)$ is spanned by Ae and $A(L_{\beta-})$. From the inequalities $\dim\{A(H_\rho)\}\geqq 2$, $\dim\{A(L_{\beta-})\}\leqq 1$ we may now deduce that

$$\dim\{A(H_\rho)\}=2,\quad \dim\{A(L_{\beta-})\}=1,\quad Ae\notin A(L_{\beta-}).$$

Let u_0 be an element of $L_{\beta-}$ such that $Au_0\neq 0$. We now sub-divide case 2 into two alternatives.

Alternative (a). *For some* $\mu>\alpha$, $(I-E_\mu)Au_0$, $(I-E_\mu)Ae$ *are linearly independent.* Choose $f(\neq 0)\in L_\mu$, and $u_1\in H_\rho\ominus L_\mu$, such that

$$\langle Ae,u_1\rangle=0\neq\langle Au_0,u_1\rangle.$$

We then define

$$Bx = \langle x, u_1\rangle f, \qquad Cx = \langle x, e\rangle e \qquad\qquad (x \in H_\rho),$$

and may verify that $B, C \in \mathcal{J}_\rho$, that $BAC = 0$, but that $BA \neq 0 \neq AC$.

Alternative (b). *For each* $\mu > \alpha$, $(I - E_\mu)Au_0$, $(I - E_\mu)Ae$ *are linearly dependent.* We may deduce, by the type of argument used in case 1 alternative (b), that $(I - E_\alpha)Au_0$, $(I - E_\alpha)Ae$ are linearly dependent. Hence there is a linear combination u_1 of e and u_0 such that $0 \neq Au_1 = E_\alpha Au_1$; and by following the method of case 1 alternative (b), we may construct $u_2 (\in H_\rho)$ such that $E_\alpha Au_2 = 0 \neq Au_2$. We define $B = E_\alpha$, $Cx = \langle x, e\rangle u_2$ $(x \in H_\rho)$. Once again we may verify that $B, C \in \mathcal{J}_\rho$, that $BAC = 0$, but that $BA \neq 0 \neq AC$.

The four situations considered above are jointly exhaustive, and in each, the assumption that A has rank exceeding unity leads to a proof that condition (ii) of the lemma is not satisfied. Hence the two stated conditions are fulfilled if and only if A has rank unity. Since these conditions are obviously invariant under algebraic isomorphism, the lemma is proved.

LEMMA 5. *Let* $\mathcal{J}$ *be an ordered basis over a separable Hilbert space* H, *and suppose that* $T \in \mathcal{J}$. *If* $ST = 0$ *whenever* $S \in \mathcal{J}$ *and* S *has rank unity, then* $T = 0$.

Proof. It is again sufficient to consider the case in which $\mathcal{J} = \mathcal{J}_\rho$, where ρ is some non-negative measure defined on the Borel subsets of $[0, 1]$. Suppose that $T \neq 0$, and choose $u (\in H_\rho)$ such that $Tu \neq 0$. We consider two cases. In the following, α is defined as in the proof of Lemma 4.

Case 1. *For some* $\lambda > \alpha$, $(I - E_\lambda)Tu \neq 0$. Choose $f (\neq 0)$ such that $f = E_\lambda f$, and define $Sx = \langle x, (I - E_\lambda)Tu\rangle f$ $(x \in H_\rho)$. Then we may verify by means of Lemma 3 that $S \in \mathcal{J}_\rho$. Furthermore, S has rank unity and $STu \neq 0$.

Case 2. *For every* $\lambda > \alpha$, $(I - E_\lambda)Tu = 0$. Then $(I - E_\alpha)Tu = 0$, and thus $E_\alpha \neq 0$. If we now set $S = E_\alpha$, it follows that S is an operator of rank unity, and that $STu = Tu \neq 0$.

The two cases considered above are jointly exhaustive, and in each of them the assumption that $T \neq 0$ leads to the construction of an operator S of rank unity such that $S \in \mathcal{J}_\rho$ and $ST \neq 0$. Hence the lemma is proved.

LEMMA 6. *Let* $\mathcal{J}_1$, $\mathcal{J}_2$ *be ordered bases over separable Hilbert spaces* H_1, H_2 *respectively. Let* ϕ, ψ *be two algebraic isomorphisms from* $\mathcal{J}_1$ *onto* $\mathcal{J}_2$ *such that* $\phi(S) = \psi(S)$ *whenever* $S \in \mathcal{J}_1$ *and* S *has rank unity. Then* $\phi = \psi$.

Proof. Let $T \in \mathfrak{I}_1$, and define $T' = \phi(T) - \psi(T)$. Let S' be any operator of rank unity in $\mathfrak{I}_2$. We may set $S' = \phi(S)$, where $S \in \mathfrak{I}_1$ and (by virtue of Lemma 4) S has rank unity. Hence the operators S, ST have rank at most unity, and we have

$$\begin{aligned} \psi(S) &= \phi(S) = S', \\ 0 &= \phi(ST) - \psi(ST) \\ &= \phi(S)\phi(T) - \psi(S)\psi(T) \\ &= S'\{\phi(T) - \psi(T)\} \\ &= S'T'. \end{aligned}$$

This holds whenever $S' \in \mathfrak{I}_2$ and S' has rank unity. Lemma 5 now implies that $T' = 0$, that is, $\phi(T) = \psi(T)$. Since T is an arbitrary element of $\mathfrak{I}_1$, we have $\phi = \psi$.

4. Diagonal isomorphisms from an ordered basis onto itself. Let $\mathfrak{I}$ be an ordered basis over a separable Hilbert space H, with diagonal $\mathfrak{A}$. By a *diagonal isomorphism on* $\mathfrak{I}$ we shall mean an algebraic isomorphism ϕ from $\mathfrak{I}$ onto itself, such that $\phi(A) = A$ $(A \in \mathfrak{A})$.

THEOREM 1. *Let $\mathfrak{I}$ be an ordered basis over a separable Hilbert space H, with diagonal $\mathfrak{A}$, and let ϕ be a diagonal isomorphism on $\mathfrak{I}$. Then ϕ is a spatial isomorphism, and may be implemented by a non-singular transformation belonging to the diagonal $\mathfrak{A}$.*

Remark. For the case in which the ordered basis $\mathfrak{I}$ has an atomic diagonal, this result is contained in Theorem 3.2.3 of [3].

Proof. We may suppose without loss of generality that $\mathfrak{I}$ is the ordered basis $\mathfrak{I}_\rho$ described in § 2. We define

$$\alpha = \sup\{\lambda : \rho([0,\lambda]) = 0\}, \qquad \beta = \inf\{\lambda : \rho([\lambda,1]) = 0\}.$$

It is clear that $\rho([0,\alpha)) = 0 = \rho((\beta,1])$. We may ignore the trivial case in which the measure ρ is concentrated on a single point (and H_ρ is one-dimensional), and deduce that $\beta > \alpha$. By a linear transformation on the real numbers we may reduce to the case in which $\beta = 1$, $\alpha = 0$. Thus we have $H = H_\rho$, $\mathfrak{I} = \mathfrak{I}_\rho$, and

$$\rho([0,\lambda]) \neq 0 \neq \rho([\lambda,1]) \qquad (0 < \lambda < 1), \tag{1}$$

$$E_\lambda \neq 0 \neq I - E_{\lambda-} \qquad (0 < \lambda < 1). \tag{2}$$

The remainder of the proof is divided into a number of sections.

(a) *Proper dissection-points.* These are the points $\lambda(\in[0,1])$ such that both the intervals $[0,\lambda]$, $[\lambda,1]$ have positive ρ-measure. Under our assumptions, every interior point of $[0,1]$ is a proper dissection point: an end-point of $[0,1]$ is a proper dissection point if and only if it has positive ρ-measure. Hence the proper dissection points form an interval X such that

$$(0,1)\subset X\subset[0,1], \qquad \rho(X)=\rho([0,1]). \tag{3}$$

(b) *The functions $a(t)$, $b(t)$.* When $e,f\in H_\rho$, we denote by $e\otimes f$ the linear operator S from H_ρ into itself which is defined by $Sx=\langle x,e\rangle f$ $(x\in H_\rho)$. When τ is a Borel subset of $[0,1]$, we write $\chi_\tau=\chi_\tau(t)$ for the characteristic function of τ.

Given a proper dissection point λ, we may consider the operator $F_\lambda=\chi_{[\lambda,1]}\otimes\chi_{[0,\lambda]}$. This operator has rank unity, and it is immediate from Lemma 3 that $F_\lambda\in\mathfrak{J}_\rho$. It is easily verified that

$$F_\lambda=E_\lambda F_\lambda(I-E_{\lambda-}).$$

By applying the diagonal isomorphism ϕ, which leaves invariant the operators $I,E_\lambda,E_{\lambda-}\in\mathfrak{A}_\rho$, we obtain

$$\phi(F)=E_\lambda\phi(F_\lambda)(I-E_{\lambda-}). \tag{4}$$

From Lemma 4 it follows that the operator $\phi(F_\lambda)$ has rank unity; we may set

$$\phi(F_\lambda)=a_\lambda\otimes b_\lambda,$$

where a_λ, b_λ are non-zero elements of H_ρ, and are determined to within scalar factors ζ, η (respectively) such that $\bar{\zeta}\eta=1$. From (4) it follows that (possibly after modifying a_λ, b_λ on ρ-null sets) we have

$$\begin{aligned} a_\lambda(t)&=0 \quad (t<\lambda),\\ b_\lambda(t)&=0 \quad (t>\lambda). \end{aligned} \tag{5}$$

Our immediate objective is to show that, if a_λ and b_λ are suitably normalised, then we have

$$a_\lambda(t)=\chi_{[\lambda,1]}(t)a(t), \qquad b_\lambda(t)=\chi_{[0,\lambda]}(t)b(t) \qquad\qquad (\lambda\in X),$$

where a and b are fixed ρ-measurable functions.

Suppose therefore that $\mu,\lambda\in X$ and $\mu\geqq\lambda$. We have

$$\begin{aligned} 0&\neq\chi_{[\mu,1]}\otimes\chi_{[0,\lambda]}\\ &=(\chi_{[\lambda,1]}\otimes\chi_{[0,\lambda]})(I-E_{\mu-})\\ &=E_\lambda(\chi_{[\mu,1]}\otimes\chi_{[0,\mu]}). \end{aligned}$$

By applying the diagonal isomorphism ϕ we obtain

$$(a_\lambda \otimes b_\lambda)(I - E_{\mu-}) = E_\lambda(a_\mu \otimes b_\mu) \neq 0,$$

that is

$$(\chi_{[\mu,1]}a_\lambda) \otimes b_\lambda = a_\mu \otimes (\chi_{[0,\lambda]}b_\mu) \neq 0. \tag{6}$$

We now choose and fix a proper dissection point α. If $\lambda \in X$ and $\lambda \leqq \alpha$, we consider equation (6), with μ replaced by α. If $\lambda \in X$ and $\lambda \geqq \alpha$, we consider equation (6), with λ, μ replaced (respectively) by α, λ. We conclude that the functions a_λ, b_λ may be normalized in such a way that, with the possible exception of certain sets of ρ-measure zero, we have

$$\left.\begin{aligned} a_\lambda(t) &= a_\alpha(t)\chi_{[\lambda,1]}(t) \\ \chi_{[0,\alpha]}(t)b_\lambda(t) &= b_\alpha(t) \end{aligned}\right\} \quad (\lambda \in X, \lambda \geqq \alpha), \tag{7}$$

$$\left.\begin{aligned} \chi_{[\alpha,1]}(t)a_\lambda(t) &= a_\alpha(t) \\ b_\lambda(t) &= b_\alpha(t)\chi_{[0,\lambda]}(t) \end{aligned}\right\} \quad (\lambda \in X, \lambda \leqq \alpha). \tag{8}$$

Having normalised the functions a_λ, b_λ $(\lambda \in X)$ by means of equations (7), (8), we remark that

$$\left.\begin{aligned} a_\mu(t) &= a_\lambda(t)\chi_{[\mu,1]}(t) \\ \chi_{[0,\lambda]}(t)b_\mu(t) &= b_\lambda(t) \end{aligned}\right\} \quad (\lambda, \mu \in X, \lambda \leqq \mu), \tag{9}$$

with the possible exception of certain ρ-null sets. The existence of *some* normalisation of the functions a_λ, a_μ, b_λ, b_μ for which (9) is valid is an immediate consequence of (6). To prove the validity of (9) for the particular normalisation given by (7), (8), we note that both $a_\mu(t)$, $a_\lambda(t)$ are equal to $a_\alpha(t)$ at almost all points of the interval $[\max(\mu, \lambda, \alpha), 1]$: and that the three functions do not vanish at almost all points of this interval (since otherwise, in view of (5), one of them would be a ρ-null function, contrary to hypothesis). Hence the normalisation for which (9) is valid coincides with that defined by (7) and (8).

We now choose an increasing sequence of closed intervals $X_n = [\lambda_n, \mu_n]$ whose union is X, and define

$$a(t) = \begin{cases} a_{\lambda_1}(t) & (\lambda_1 \leqq t \leqq 1), \\ a_{\lambda_n}(t) & (\lambda_n \leqq t < \lambda_{n-1} : n > 1); \end{cases}$$

$$b(t) = \begin{cases} b_{\mu_1}(t) & (0 \leqq t \leqq \mu_1), \\ b_{\mu_n}(t) & (\mu_{n-1} < t \leqq \mu_n : n > 1). \end{cases}$$

The functions $a(t)$, $b(t)$ are defined throughout X, and hence at almost all points of $[0,1]$. From (9) we deduce that, with the possible exception of certain ρ-null sets, we have

$$\left.\begin{aligned} a_\lambda(t) &= a(t)\chi_{[\lambda,1]}(t), \\ b_\lambda(t) &= b(t)\chi_{[0,\lambda]}(t) \end{aligned}\right\} \quad (\lambda \in X). \tag{10}$$

Finally, we deduce from the defining property of the functions a_λ, b_λ, and from equations (10), that

$$\phi(\chi_{[\lambda,1]}\otimes\chi_{[0,\lambda]}) = (a\chi_{[\lambda,1]}\otimes b\chi_{[0,\lambda]}) \qquad (\lambda\in X). \tag{11}$$

(c) *The relation* $b(t)\overline{a(t)}=1$. Let $\lambda,\mu\in X$ and suppose that $\lambda\leqq\mu$. An elementary calculation shows that

$$(\chi_{[\lambda,\mu]}\otimes\chi_{[0,\lambda]})\ (\chi_{[\mu,1]}\otimes\chi_{[\lambda,\mu]}) = \rho([\lambda,\mu])\,(\chi_{[\mu,1]}\otimes\chi_{[0,\lambda]}).$$

This relation may be re-written in the form

$$\begin{aligned}(\chi_{[\lambda,1]}\otimes\chi_{[0,\lambda]})E_\mu.\ (I-E_{\lambda-})\ (\chi_{[\mu,1]}\otimes\chi_{[0,\mu]})&\\ =\rho([\lambda,\mu])E_\lambda(\chi_{[\mu,1]}\otimes\chi_{[0,\mu]})&.\end{aligned}$$

If we apply the diagonal isomorphism ϕ to the last equation, and use (11), we obtain

$$\begin{aligned}(a\chi_{[\lambda,1]}\otimes b\chi_{[0,\lambda]})E_\mu.\ (I-E_{\lambda-})\ (a\chi_{[\mu,1]}\otimes b\chi_{[0,\mu]})&\\ =\rho([\lambda,\mu])E_\lambda(a\chi_{[\mu,1]}\otimes b\chi_{[0,\mu]})&,\end{aligned}$$

that is

$$(a\chi_{[\lambda,\mu]}\otimes b\chi_{[0,\lambda]})\,(a\chi_{[\mu,1]}\otimes b\chi_{[\lambda,\mu]}) = \rho([\lambda,\mu])\,(a\chi_{[\mu,1]}\otimes b\chi_{[0,\lambda]}). \tag{12}$$

An elementary calculation shows that the left hand side of (12) is equal to

$$\left(\int_{[\lambda,\mu]} b(t)\overline{a(t)}\,d\rho(t)\right)(a\chi_{[\mu,1]}\otimes b\chi_{[0,\lambda]}).$$

Since, as has been verified in the above calculations,

$$(a\chi_{[\mu,1]}\otimes b\chi_{[0,\lambda]}) = \phi(\chi_{[\mu,1]}\otimes\chi_{[0,\lambda]})\neq 0,$$

we deduce that

$$\int_{[\lambda,\mu]} b(t)\overline{a(t)}\,d\rho(t) = \rho([\lambda,\mu]) \qquad (\lambda,\mu\in X:\ \lambda\leqq\mu).$$

It follows that $b(t)\overline{a(t)}=1$ at almost all points of X, and hence at almost all points of $[0,1]$.

(d) *Proof that a, b are ρ-essentially bounded.* Suppose that $f,g\in H_\rho$, that $\lambda\in X$, and that the functions $\bar{f}\chi_{[\lambda,1]}$, $g\chi_{[0,\lambda]}$ are not ρ-null functions. Then the operator $\bar{f}\chi_{[\lambda,1]}\otimes g\chi_{[0,\lambda]}$ has rank unity, and is a member of $\mathfrak{F}_\rho$. We define

$$f_1=1/(1+|f|),\qquad f_2=f/(1+|f|),$$
$$g_1=1/(1+|g|),\qquad g_2=g/(1+|g|).$$

Then f_1, f_2, g_1, g_2 are ρ-essentially bounded measurable functions. With these we associate the corresponding multiplication operators $M_{f_1}, \cdots, M_{g_2}$, which belong to the diagonal $\mathcal{A}_\rho$ of the ordered basis $\mathcal{J}_\rho$. From the (easily verified) formula

$$M_{h_1}(\bar{h}_2 \otimes h_3)M_{h_4} = (\bar{h}_4\bar{h}_2) \otimes (h_1h_3) \qquad (h_1, h_4 \in L^\infty([0,1]:\rho)\,; h_2, h_3 \in H_\rho),$$

and the relations $ff_1 = f_2$, $gg_1 = g_2$, we deduce that

$$M_{g_1}(\bar{f}\chi_{[\lambda,1]} \otimes g\chi_{[0,\lambda]})M_{f_1} = M_{g_2}(\chi_{[\lambda,1]} \otimes \chi_{[0,\lambda]})M_{f_2}. \tag{13}$$

Let us now operate on equation (13) with the diagonal isomorphism ϕ. We may suppose that

$$\phi(\bar{f}\chi_{[\lambda,1]} \otimes g\chi_{[0,\lambda]}) = \bar{F} \otimes G,$$

where F, G are non-zero elements of H_ρ. We obtain

$$M_{g_1}(\bar{F} \otimes G)M_{f_1} = M_{g_2}(a\chi_{[\lambda,1]} \otimes b\chi_{[0,\lambda]})M_{f_2},$$

that is

$$(\bar{f}_1\bar{F}) \otimes (g_1G) = (a\bar{f}_2\chi_{[\lambda,1]}) \otimes (bg_2\chi_{[0,\lambda]}).$$

It follows that F and G may be normalised in such a way that (with the possible exception of certain ρ-null sets)

$$f_1F = \bar{a}f_2\chi_{[\lambda,1]},$$
$$g_1G = bg_2\chi_{[0,\lambda]}.$$

Hence

$$F = \bar{a}f\chi_{[\lambda,1]},$$
$$G = bg\chi_{[0,\lambda]}.$$

We deduce that $\bar{a}f\chi_{[\lambda,1]}$, $bg\chi_{[0,\lambda]} \in H_\rho$, and that

$$\phi(\bar{f}\chi_{[\lambda,1]} \otimes g\chi_{[0,\lambda]}) = (a\bar{f}\chi_{[\lambda,1]}) \otimes (bg\chi_{[0,\lambda]}). \tag{14}$$

It is apparent that this equation remains valid when one or both of $\bar{f}\chi_{[\lambda,1]}$, $g\chi_{[0,\lambda]}$ is a ρ-null function.

We now choose a proper dissection point λ, and an element f of H_ρ, such that $f(t) \neq 0$ $(0 \leqq t \leqq 1)$. We keep f and λ fixed, but allow g to vary in H_ρ. Since ϕ is an algebraic isomorphism from $\mathcal{J}_\rho$ onto itself, and preserves the property of being of rank unity, we deduce from equation (14) that as g runs through H_ρ, $bg\chi_{[0,\lambda]}$ runs through all elements of H_ρ which vanish on the interval $(\lambda, 1]$. It follows that both b and its inverse function b^{-1} are ρ-essentially bounded on $[0,\lambda]$. Similar considerations show that a and a^{-1} are ρ-essentially bounded on $[\lambda, 1]$. Since $b\bar{a} = 1$, we may deduce that a, a^{-1} are ρ-essentially bounded on $[0,1]$.

(e) *Conclusion of the proof of Theorem* 1. Equation (14) may be written in the form

$$(15)\qquad \phi(\bar{f}\chi_{[\lambda,1]}\otimes g\chi_{[0,\lambda]}) = M_b(\bar{f}\chi_{[\lambda,1]}\otimes g\chi_{[0,\lambda]})M_{\bar{a}} = Q^{-1}(\bar{f}\chi_{[\lambda,1]}\otimes g\chi_{[0,\lambda]})Q,$$

where Q ($\in \mathcal{A}_\rho$) is the operator $M_{\bar{a}}$. It follows from Lemma 3 that every operator of rank unity in $\mathcal{J}_\rho$ can be written in the form $\bar{f}\chi_{[\lambda,1]}\otimes g\chi_{[0,\lambda]}$ for some $\lambda \in X$. From (15) we deduce that ϕ coincides, in its action on operators of rank unity, with the spatial isomorphism induced by Q. It now follows from Lemma 6 that ϕ coincides with this spatial isomorphism. This completes the proof of Thorem 1.

5. Symmetric isomorphisms between ordered bases.

Let $\mathcal{J}_i$ be an ordered basis over a separable Hilbert space H_i, with diagonal $\mathcal{A}_i$ ($i = 1, 2$). By a *symmetric isomorphism* from $\mathcal{J}_1$ onto $\mathcal{J}_2$ we shall mean an algebraic isomorphism ϕ from $\mathcal{J}_1$ onto $\mathcal{J}_2$ such that $\phi(A^*) = \phi(A)^*$ ($A \in \mathcal{A}_1$).

THEOREM 2. *Let $\mathcal{J}_i$ be an ordered basis over a separable Hilbert space H_i, with diagonal $\mathcal{A}_i$ ($i = 1, 2$), and let ϕ be a symmetric isomorphism from $\mathcal{J}_1$ onto $\mathcal{J}_2$. Then ϕ is a spatial isomorphism, and may be implemented by a transformation of the form $Q = Q_1U$, where U is a unitary operator from H_2 onto H_1 and $Q_1 \in \mathcal{A}_1$.*

Remark. For the case in which each of the ordered bases has atomic diagonal, this result is contained in Theorem 3.2.3 of [3]. I am indebted to Professor R. V. Kadison for a suggestion which has enabled me to shorten substantially the arguments by which Theorem 2 is deduced from Theorem 1.

Proof. Let $A \in \mathcal{A}_1$. Then $A, A^* \in \mathcal{J}_1$ and we have

$$\phi(A) \in \mathcal{J}_2, \qquad \phi(A)^* = \phi(A^*) \in \mathcal{J}_2.$$

It follows that $\phi(A) \in \mathcal{A}_2$, and that $\phi(\mathcal{A}_1) \subset \mathcal{A}_2$. Since $\phi(\mathcal{A}_1)$ is a maximal abelian sub-algebra of $\mathcal{J}_2$, while $\mathcal{A}_2$ is abelian, we may deduce that $\phi(\mathcal{A}_1) = \mathcal{A}_2$. Thus ϕ induces an adjoint-preserving algebraic isomorphism from $\mathcal{A}_1$ onto $\mathcal{A}_2$; and $\mathcal{A}_i$ is a maximal abelian self-adjoint sub-algebra of (H_i, H_i) ($i = 1, 2$). It follows (see the uniqueness clause of Theorem 5 of [5]) that there is a unitary operator U from H_2 onto H_1 such that

$$(16)\qquad \phi(A) = U^{-1}AU \qquad (A \in \mathcal{A}_1).$$

We shall now prove that

$$(17)\qquad \mathcal{J}_2 = U^{-1}\mathcal{J}_1U.$$

For let $\mathcal{F}_1$ be the family of all hull projections in $\mathcal{J}_1$. Then $\mathcal{F}_1 \subset \mathcal{A}_1$, and $\mathcal{F}_1$ is a full set of hull idempotents for $\mathcal{J}_1$. If we now define

$$\mathcal{F}_2 = \phi(\mathcal{F}_1) = U^{-1}\mathcal{F}_1 U, \tag{18}$$

it follows from Lemma 2 that $\mathcal{F}_2$ is a full set of hull idempotents for $\mathcal{J}_2$. Hence, for $i = 1, 2$, $\mathcal{J}_i$ consists of all operators S which act in H_i and satisfy $SE = ESE$ $(E \in \mathcal{F}_i)$. From (18) it is immediate that $\mathcal{J}_2 = U^{-1}\mathcal{J}_1 U$. This proves (17).

We now define

$$\psi(S) = U\phi(S)U^{-1} \qquad (S \in \mathcal{J}_1). \tag{19}$$

From (16) and (17) we deduce that ψ is an algebraic isomorphism from $\mathcal{J}_1$ onto itself, and that $\psi(A) = A$ $(A \in \mathcal{A}_1)$. Thus ψ is a diagonal isomorphism from $\mathcal{J}_1$ onto itself, and (by Thesorem 1) is a spatial isomorphism which may be implemented by an operator Q_1 $(\in \mathcal{A}_1)$. Hence

$$\psi(S) = Q_1^{-1}SQ_1 \qquad (S \in \mathcal{J}_1),$$

and

$$\begin{aligned}\phi(S) &= U^{-1}\psi(S)U \\ &= U^{-1}Q_1^{-1}SQ_1U \\ &= Q^{-1}SQ \qquad (S \in \mathcal{J}_1),\end{aligned}$$

where $Q = Q_1U$. This proves Theorem 2.

6. Algebraic isomorphisms between ordered bases.

THEOREM 3. *Let $\mathcal{J}_i$ be an ordered basis over a separable Hilbert space H_i $(i = 1, 2)$, and let ϕ be an algebraic isomorphism from $\mathcal{J}_1$ onto $\mathcal{J}_2$. Then ϕ is a spatial isomorphism.*

Proof. In view of the representation theorem stated in § 2, it is sufficient to consider the case in which $\mathcal{J}_1 = \mathcal{J}_\rho$, where ρ is some non-negative measure defined on the Borel subsets of $[0, 1]$. We shall use the notations introduced in § 2. The proof is divided into a number of stages.

(a) Consider the algebra $\phi(\mathcal{A}_\rho)$. This is a maximal abelian sub-algebra of $\mathcal{J}_2$, and since $\mathcal{J}_2$ is weakly closed, the same is true of $\phi(\mathcal{A}_\rho)$. A fortiori $\phi(\mathcal{A}_\rho)$ is uniformly closed and, with operator bound as norm, forms a commutative Banach algebra. Thus ϕ induces an algebraic isomorphism ψ from the commutative von Neumann algebra $\mathcal{A}_\rho$ onto the commutative Banach algebra $\phi(\mathcal{A}_\rho)$. It is clear, from the definition

$$r_A = \inf\{\mu \colon \mu > 0, |\lambda| > \mu \Rightarrow \lambda I - A \text{ has an inverse in } \mathcal{J}\}$$

of the *spectral radius* r_A of an element A in a Banach algebra $\mathfrak{J}$, that ψ preserves spectral radius. Now

$$r_A = \| A \| \qquad (A \in \mathfrak{A}_\rho),$$

since $\mathfrak{A}_\rho$ consists of normal operators; and

$$r_{\psi(A)} \leqq \| \psi(A) \| \qquad (A \in \mathfrak{A}_\rho),$$

by a well known inequality (see, for example, [2], p. 567, Lemma 4). Thus we have

$$\| A \| = r_A = r_{\psi(A)} \leqq \| \psi(A) \| \qquad (A \in \mathfrak{A}_\rho).$$

Hence (considering $\mathfrak{A}_\rho$ and $\phi(\mathfrak{A}_\rho)$ as Banach spaces) ψ^{-1} is a continuous linear operator from $\phi(\mathfrak{A}_\rho)$ onto $\mathfrak{A}_\rho$. The inversion theorem (see, for example, [2], p. 57, Theorem 2) implies that ψ is also continuous. We may therefore choose a constant K such that

$$(20) \qquad \| A \| \leqq \| \phi(A) \| \leqq K \| A \| \qquad (A \in \mathfrak{A}_\rho).$$

(b) Let $E(\tau)$ be the spectral measure in $\mathfrak{A}_\rho$, and let E_λ, $E_{\lambda-}$ be defined as in § 2. We set

$$(21) \qquad \begin{aligned} F(\tau) &= \phi(E(\tau)), \\ F_\lambda &= \phi(E_\lambda), \\ F_{\lambda-} &= \phi(E_{\lambda-}) \end{aligned}$$

for all Borel subsets τ of $[0,1]$ and all $\lambda \in [0,1]$. It is immediate that

$$(22) \qquad F_\lambda = F([0,\lambda]), \quad F_{\lambda-} = F([0,\lambda)) \qquad (0 \leqq \lambda \leqq 1).$$

Furthermore, if τ, τ_1, τ_2 are Borel subsets of $[0,1]$, τ_0 is the empty set, and K is the constant occuring in (20), we have

(i) $F(\tau_0) = 0, \quad F([0,1]) = I;$

(ii) $F(\tau_1 \cap \tau_2) = F(\tau_1)F(\tau_2),$
$F(\tau_1 \cup \tau_2) = F(\tau_1) + F(\tau_2)$ provided $\tau_1 \cap \tau_2 = \tau_0$;

(iii) $\| F(\tau) \| \leqq K.$

Conditions (i), (ii) follow from the corresponding properties of $E(\tau)$, and (iii) is seen to be a consequence of (20) and (21) when we recall that $E(\tau) \in \mathfrak{A}_\rho$ and that $\| E(\tau) \| \leqq 1$.

We may now deduce from a theorem of Dixmier ([1], p. 222: see also [4], [6]) that it is possible to find a Hilbert space H_3, and a one to one bicontinuous linear operator P from H_3 onto H_2, such that

$$(23) \qquad G(\tau) = P^{-1}F(\tau)P$$

is a self-adjoint operator for each Borel subset τ of $[0,1]$. It is clear that H_3 is separable.

(c) We define

$$\mathcal{J}_3 = P^{-1}\mathcal{J}_2 P, \qquad \mathcal{A}_3 = P^{-1}\phi(\mathcal{A}_\rho)P.$$

We shall prove that $\mathcal{J}_3$ is an ordered basis with diagonal $\mathcal{A}_3$.

Since the operators E_λ, $E_{\lambda-}$ $(0 \leqq \lambda \leqq 1)$ form a full set of hull idempotents for $\mathcal{J}_\rho$, it follows from Lemma 2 and from equations (21) that F_λ, $F_{\lambda-}$ $(0 \leqq \lambda \leqq 1)$ are a full set of hull idempotents for $\mathcal{J}_2$. Hence $\mathcal{J}_2$ consists of all operators acting in H_2 which leave invariant the ranges of the idempotents F_λ, $F_{\lambda-}$ $(0 \leqq \lambda \leqq 1)$. Thus, if we define

$$(24) \qquad G_\lambda = P^{-1}F_\lambda P, \qquad G_{\lambda-} = P^{-1}F_{\lambda-}P,$$

then $\mathcal{J}_3$ consists of all operators acting in H_3 which leave invariant the ranges of the idempotents G_λ, $G_{\lambda-}$ $(0 \leqq \lambda \leqq 1)$. Hence

$$(25) \quad \mathcal{J}_3 = \{T \in (H_3, H_3) : TG_\lambda = G_\lambda T G_\lambda,\ TG_{\lambda-} = G_{\lambda-} T G_{\lambda-} \ (0 \leqq \lambda \leqq 1)\}.$$

From equations (22), (23) and (24) we deduce that $G_\lambda = G([0,\lambda])$, $G_{\lambda-} = G([0,\lambda))$. Hence the idempotents G_λ, $G_{\lambda-}$ $(0 \leqq \lambda \leqq 1)$ are projections, and in fact form a linearly ordered family of projections. If we now prove that the von Neumann algebra $\mathcal{B}_3$ generated by these projections is a maximal abelian sub-algebra of $(\mathrm{H}_3, \mathrm{H}_3)$, we shall be able to deduce from Theorem 3.1.1 of [3] that $\mathcal{J}_3$ is an ordered basis with diagonal $\mathcal{B}_3$.

When $S \in \mathcal{J}_\rho$ we define

$$(26) \qquad \psi(S) = P^{-1}\phi(S)P.$$

Thus ψ is an algebraic isomorphism from $\mathcal{J}_\rho$ onto $\mathcal{J}_3$, and

$$(27) \qquad \psi(\mathcal{A}_\rho) = P^{-1}\phi(\mathcal{A}_\rho)P = \mathcal{A}_3.$$

Furthermore,

$$(28) \qquad \psi(E_\lambda) = G_\lambda, \qquad \psi(E_{\lambda-}) = G_{\lambda-} \qquad (0 \leqq \lambda \leqq 1).$$

Let $\mathcal{B}'_3$ denote the commutant of $\mathcal{B}_3$. Then

$$\mathcal{B}'_3 = \{T \in (H_3, H_3) : TG_\lambda = G_\lambda T, \qquad TG_{\lambda-} = G_{\lambda-}T \qquad (0 \leqq \lambda \leqq 1)\}.$$

It is clear from (25), and the preceding line, that $\mathcal{B}'_3 \subset \mathcal{J}_3$; hence

$$\begin{aligned}\mathcal{B}'_3 &= \{T \in \mathcal{J}_3 : TG_\lambda = G_\lambda T, TG_{\lambda-} = G_{\lambda-}T \ (0 \leqq \lambda \leqq 1)\}\\ &= \psi(\{S \in \mathcal{J}_\rho : SE_\lambda = E_\lambda S, SE_{\lambda-} = E_{\lambda-}S \ (0 \leqq \lambda \leqq 1)\})\\ &= \psi(\mathcal{A}_\rho)\\ &= \mathcal{A}_3.\end{aligned}$$

Thus $\mathfrak{B}'_3$ is abelian, and contains $\mathfrak{B}_3$ (since $G_\lambda, G_{\lambda-} \in \mathfrak{A}_3$). Since, by the double commutant theorem, $\mathfrak{B}_3 = \mathfrak{B}''_3$, we deduce that $\mathfrak{B}_3 = (\mathfrak{B}'_3)' \subset \mathfrak{B}'_3$. Hence $\mathfrak{B}_3 = \mathfrak{B}'_3 = \mathfrak{A}_3$. It easily follows that $\mathfrak{B}_3$ $(= \mathfrak{A}_3)$ is a maximal abelian sub-algebra of (H_3, H_3), and hence that $\mathfrak{F}_3$ is an ordered basis with diagonal $\mathfrak{A}_3$.

(d) From (20) and (26) it follows that ψ, as a mapping from $\mathfrak{A}_\rho$ onto $\mathfrak{A}_3$, is continuous if each of these algebras is considered with its uniform topology. Since

$$\psi(E(\tau)) = G(\tau),$$

we deduce that ψ is adjoint-preserving on the uniformly closed sub-algebra of $\mathfrak{A}_\rho$ which is generated by the projections $E(\tau)$. But this sub-algebra is in fact the whole of $\mathfrak{A}_\rho$ (as follows from the spectral theorem for normal operators, or by elementary arguments based on the fact that $\mathfrak{A}_\rho$ is a multiplication algebra). Hence

$$\psi(T^*) = \psi(T)^* \qquad (T \in \mathfrak{A}_\rho).$$

Thus ψ is a symmetric isomorphism from $\mathfrak{F}_\rho$ onto $\mathfrak{F}_3$, and, by Theorem 2, is spatial. From equation (26) it is now immediate that ϕ is spatial. This proves Theorem 3.

UNIVERSITY OF DURHAM,
KING'S COLLEGE,
NEWCASTLE UPON TYNE 2, ENGLAND.

REFERENCES.

[1] J. Dixmier, "Les moyennes invariantes dans les semi-groupes et leurs applications," *Acta Scientiarum Mathematicarum Szeged*, vol. 12, Pars A (1950), pp. 213-227.

[2] N. Dunford and J. T. Schwartz, *Linear operators*, vol. 1, New York (1958).

[3] R. V. Kadison and I. M. Singer, "Triangular operator algebras," *American Journal of Mathematics*, vol. 82 (1960), pp. 227-259.

[4] G. W. Mackey, *Commutative Banach algebras*, Theorem 55; multigraphed Harvard lecture notes, edited by A. Blair (1952).

[5] I. E. Segal, "Decompositions of operator algebras II," *Memoirs of the American Mathematical Society*, no. 9 (1951).

[6] J. Wermer, "Commuting spectral measures on Hilbert space," *Pacific Journal of Mathematics*, vol. 4 (1954), pp. 355-361.

SOME GLOBAL PROBLEMS IN THE THEORY OF FUNCTIONS OF SEVERAL COMPLEX VARIABLES.*

By ERRETT BISHOP.[1]

1. **Introduction.** In a previous paper [2] the global structure of a complex analytic variety was examined in some detail. The present paper is a sequel containing some application of those results. In order that this paper be self-contained, the definitions and results of [2] are summarized in Section 2.

Consider now an analytic subset L of a Stein manifold K. It is a consequence of Theorems A and B of [3] that

I. The set L is the set of common zeros of some family Γ of analytic functions on K.

II. If L is a submanifold of K then every analytic function on L can be extended to an analytic function on K.

Previous work on Problems I and II was done by Oka [5], [6], and others. In Section 3 we give new proofs of I and II which are independent of sheaf theory. The proof of I contains an explicit formula for the functions in the class Γ, and in this respect gives information which is not available from the sheaf-theoretic proof. Similarly the proof of II contains a specific formula for the extension of a function analytic on L to a function analytic on K. This formula makes it clear that II continues to hold for analytic functions whose values lie in a Banach space, thus answering a question posed by H. Rossi in a conversation with the author.

In Section 4 we prove that the first cohomology group of the sheaf of germs of holomorphic functions on a Stein manifold is trivial. Again this result follows from sheaf theory [3]. Previous work was done by Cousin [4], Oka [5], [6], [7], and others. Since it is the purpose of this paper to proceed independently of sheaf theory, this result is formulated and proved without mention of sheaves or cohomology. As is well-known, the solutions to Cousin's first and second problems are consquences of this result.

The techniques which we use for solving these problems are all essentially similar. Since all of the problems considered have previously been solved,

---

* Received December 27, 1960.

[1] This work was supported by the Sloan Foundation and the National Science Foundation.

we have not attempted to push the theory to the limit of its generality. It should however be clear to someone familiar with the subject that the methods employed here are capable of handling the same problems in greater generality. These methods, which seem not to afford so powerful a general approach to these questions as does the theory of sheaves, nevertheless have the advantages of explicitness and simplicity. The gain in explicitness comes from the use of explicit formulas to construct the various analytic functions which arise. These formulas make it clear, for instance, that all of the above mentioned results hold for Banach space valued analytic functions.

2. Preliminaries.

In order not to burden the exposition with too much generality (as was done in [2]), we confine our attention to Stein manifolds, merely remarking that there are obvious possibilities for generalizing the results to one type or another of analytic space.

Definition 1. A *Stein manifold* K of dimension n is an n-dimensional separable complex analytic manifold K having the following properties, where $A(K)$ denotes the set of analytic functions on K

(a) For each pair (p, q) of distinct points in K there exists f in $A(K)$ with $f(p) \neq f(q)$.

(b) For each p in K there exist $f_1, \cdots, f_n$ in $A(K)$ which map some neighborhood of p homeomorphically onto an open set in n-dimensional complex affine space C^n.

(c) K is holomorphically convex. This means that for each compact subset S of K the set

$$\hat{S} = \{p \colon p \in K, |f(p)| \leqq \sup\{|f(q)| \colon q \in S\} \text{ for all } f \text{ in } A(K)\}$$

is compact.

We now state, for the special case of a Stein manifold, some of the definitions and results of [2].

Definition 2. Let K be a Stein manifold and L an analytic subset of K. Let $f_1, \cdots, f_k$ be functions in $A(K)$. Write

$$P_0 = \{p \in L \colon |f_i(p)| < 1, 1 \leqq i \leqq k\}.$$

Let P be an open and closed subset of P_0 such that P is a compact subset of L. Then P is called an analytic polyhedron in L defined by $f_1, \cdots, f_k$. The analytic polyhedron P is called *special* if L has the dimension k at each of its points.

THEOREM 1. *If P is an analytic polyhedron in a homogeneous-dimensional analytic subset L of a Stein manifold K, if S is a compact subset of P, and if T is a compact subset of K at each point of which each of the defining functions for P has absolute value less than* 1, *then there exists a special analytic polyhedron Q in L with*

$$S \subset Q \subset P$$

such that each of the functions defining Q has absolute value less than 1 *at each point of T. The functions defining Q can be chosen to be polynomials in the functions defining P.*

Since it is easy that a homogeneous-dimensional analytic subset L of a Stein manifold K can be exhausted by an increasing sequence of analytic polyhedra, it follows from Theorem 1 that L can be exhausted by an increasing sequence of special analytic polyhedra. Thus the study of L can be reduced for most purposes to the study of special analytic polyhedra in L. It turns out that a special analytic ployhedron P can be studied in detail by means of the map f of P into d-dimensional complex affine space C^d, where $d = \dim L$ and f is defined by

$$f(p) = (f_1(p), \cdot \cdot \cdot, f_d(p))$$

with $f_1, \cdot \cdot \cdot, f_d$ the functions which occur in the definition of the special analytic polyhedron P. Before we state the main results about special analytic polyhedra another definition is necessary.

Definition 3. Let X be a topological space. Let ${}^kX$ be the k-fold Cartesian product of X with itself. Define an equivalence relation on ${}^kX$ by taking $(x_1, \cdot \cdot \cdot, x_k) \sim (y_1, \cdot \cdot \cdot, y_k)$ to mean that $(y_1, \cdot \cdot \cdot, y_k)$ is a reordering of $(x_1, \cdot \cdot \cdot, x_k)$. Then ${}_kX$, the k-fold *unordered product* of X with itself, is the set of equivalence classes of ${}^kX$ under this relation. A set in ${}_kX$ is called *open* if and only if its inverse image in ${}^kX$ with respect to the natural map $\pi\colon {}^kX \to {}_kX$ is open. The image under π of the element $(x_1, \cdot \cdot \cdot, x_k)$ in ${}^kX$ will be denoted by $\{x_1, \cdot \cdot \cdot, x_k\}$.

The following three theorems give the fundamental facts about analytic polyhedra.

THEOREM 2. *Let P be a special analytic polyhedron in a d-dimensional subset L of a Stein manifold K, defined by functions $f_1, \cdot \cdot \cdot, f_d$ in $A(K)$. Let f be the map*

$$p \to (f_1(p), \cdot \cdot \cdot, f_d(p))$$

of K into C^d, so that $f(P) \subset E^d$, where

$$E^d = \{(z_1, \cdots, z_d) : |z_i| < 1, 1 \leqq i \leqq d\}.$$

Then there exists an integer λ, a continuous map ω from E^d into ${}_\lambda P$, and a closed nowhere dense subset H of E^d such that

(a) For all z in E^d the points $p_1, \cdots, p_\lambda$ in $\omega(z) = \{p_1, \cdots, p_\lambda\}$ are mapped by f into z.

(b) No other points in P are mapped by f into z.

(c) For all z in $E^d - H$ the points $p_1, \cdots, p_\lambda$ are distinct.

THEOREM 3. *With the conditions of Theorem 2 let J be the subset of P consisting of all regular points p of P such that the functions $f_1, \cdots, f_d$ are a coordinate set of functions at each of the points $p_1, \cdots, p_\lambda$ of $\omega(f(p)) = \{p_1, \cdots, p_\lambda\}$. Let g be a continuous function on P which is analytic at each point of J. Then g is analytic at each regular point of P. If also $g(p_1) = g(p_2)$ whenever p_1 and p_2 are points in P for which $f(p_1) = f(p_2)$ and if g_0 is a function on an open subset U of $f^{-1}(E^d)$ such that $g_0(q) = g(p)$ whenever $g \in U$, $p \in P$, and $f(p) = f(q)$, then g_0 is analytic on U and the function h on E^d for which $g = h \circ f$ is analytic on E^d.*

THEOREM 4. *Let T be a compact subset of a Stein manifold K and U a neighborhood of T such that for each p in $U - T$ there exists f in $A(K)$ with*

$$|f(p)| > \sup\{|f(q)| : q \in T\}.$$

Let $C(T)$ be the uniformly-normed Banach space of all continuous complex-valued functions on T. Let $\mathfrak{A}$ be the closure of $A(K)$ in the space $C(T)$. Then the spectrum of the Banach algebra $\mathfrak{A}$ is T. That is, to any continuous homomorphism ϕ of $\mathfrak{A}$ into the complex numbers corresponds a point p_0 in T with $\phi(f) = f(p_0)$ for all f in $\mathfrak{A}$.

The proof of Theorem 4 (Lemma 6 of [2]) was for certain special sets T, but by means of Theorem 1 one can easily approximate T by such special sets and thereby obtain Theorem 4 for T.

In order to study a d-dimensional analytic subset L of a Stein manifold K globally it is sometimes necessary to consider a map of K into C^d whose restriction to L is *almost proper*. This concept is explained in the following definition.

Definition 4. A continuous map f of a topological space X into a topological space Y is called *almost proper* if every component of $f^{-1}(S)$ is compact for every compact subset S of Y.

The following theorem is easily proved from the fact that an analytic subset of a Stein manifold can be exhausted by special analytic polyhedra.

THEOREM 5. *If L is a d-dimensional analytic subset of a Stein manifold K then K admits an analytic map into C^d whose restriction to L is almost proper. The mapping can be chosen to be non-singular on L at each point of any 0-dimensional set of regular points of L.*

The final result we shall need guarantees the existence of a function f_{d+1} which will be used as a convergence factor for constructions involving an almost proper map f of an analytic subset L of a Stein manifold.

THEOREM 6. *Let $f=(f_1,\cdots,f_d)$ be an analytic map of a Stein manifold K into C^d, whose restriction to the analytic subset L of K is almost proper. Let L have dimension d at each point. Let $\{S_k\}$ be an increasing sequence of compact subsets of L, each of which has finitely many components, the union of whose interiors is L. Let α be a function from the positive integers to the positive real numbers such that*

$$S_k\subset F_k=\{p\in L:|f_i(p)|\leqq\alpha(k),1\leqq i\leqq d\}$$

for all k. Let H_k be the union of all those components of F_k which intersect S_k. Then H_k is compact. For each positive integer k write

$$G_k=(H_{k+1}\cap F_k)-H_k.$$

Let $G_0=H_1$. Let $\{g_k\}$ be a sequence of functions in $A(K)$ and $\{\epsilon_k\}$ a sequence of positive real numbers. Then there exists f_{d+1} in $A(K)$ such that

$$|f_{d+1}(p)-g_k(p)|<\epsilon_k\qquad p\in G_k,\qquad 0\leqq k<\infty.$$

In addition f_{d+1} can be chosen to have distinct values modulo $2\pi i$ at the points of any countable subset of K.

Since it is not clear that Theorem 6 as stated follows from the results of [2], we indicate the modifications necessary in the proof of Theorem 8 of [2] to give Theorem 6. The only point in question is the convergence on K (and not just on L) of the series

$$f_{d+1}=\sum_{k=0}^{\infty}g_k$$

used to define f_{d+1} on p. 238 of [2]. To see that this series can be made to converge on K, let D be any compact subset of K, with $D=\hat{D}$. We shall show that for k sufficiently large the g_k can be chosen so that $|g_k(p)|<2^{-k}$ for all p in D. It will be clear that this can actually be achieved for any sequence of such compact sets D which exhausts K, from which the uniform convergence of the series for f_{d+1} on all compact subsets of K can be obtained. To this end it is sufficiently to show that the function τ constructed in the proof of Theorem 8 of [2] and used in the construction of g_k can be made arbitrarily small on D if k is sufficiently large. That is, we wish to find τ in $\mathfrak{A}$ which is arbitrarily close to 0 on $H_k \cup D$ and arbitrarily close to 1 on G_k.

Choose k so large that $D \cap L \subset H_k$. Thus there exists a neighborhood U in K of $T = H_k \cup G_k \cup D$ such that $H_k \cup G_k = F_k \cap U$. Clearly G_k is open in the set T. Thus to show that τ exists with the desired properties it is sufficient by Theorem 4 above to show that for each p in $U - T$ there exists h in $\mathfrak{A}$ with

$$|h(p)| > \sup\{|h(q)| : q \in T\}.$$

If $p \in U \cap L$ then $p \in L - F_k$ so that h can be taken to be one of the functions $f_1, \cdots, f_d$. Thus we need only consider the case $p \in U - L$. It is well known, and a new proof will be given below (Theorem 7), that there exists an analytic function h_1 on an arbitrary open relatively compact set $V \subset K$ such that $h_1(p) = 1$ and h_1 vanishes on $V \cap L$. Now since $D = \bar{D}$ there exists h_2 in $\mathfrak{A}$ with $h_2(p) = 1$ and $|h_1(q)h_2(q)| < 1$ for all q in D. Now if V is sufficiently large then by Runge's theorem for several complex variables (a new proof of which will be given below which does not depend on this theorem), the function h_1h_2 can be uniformly approximated on $T \cup \{p\}$ by functions h in $\mathfrak{A}$, so that h will have the desired property. This completes the proof that the desired function τ can be found.

3. Analytic sets in Stein manifolds.

We wish to prove Theorems I and II of the introduction. We first prove somewhat weaker results, I_1 and II_1 below, which are sufficient for most applications.

THEOREM 7. *Let L be an analytic subset of a Stein manifold K. Let U be an open subset of K whose closure is compact. Let L have the same dimension d at each of its points. Then*

I_1. *For each p_0 in $U - L$ there exists an analytic function h on U, defined by (*) below, which vanishes on $U \cap L$, with $h(p_0) \neq 0$.*

II_1. *If in addition L is a submanifold of K then every analytic function u on L can be extended to an analytic function $\bar{u}$ on U, given by (a), (d), and (e) below.*

Proof. Since K is a Stein manifold and $\bar{U}$ is compact there exists an analytic polyhedron Q in K with $\bar{U} \subset Q$. Thus $Q \cap L$ is an analytic polyhedron in L. By Theorem 1 there exist functions $f_1, \cdots, f_d$ in $A(K)$ defining an analytic polyhedron P in L with $U \cap L \subset P$ and $|f_i(p)| < 1$ for p in $\bar{U}$ and $1 \leqq i \leqq d$. Let f be the map

$$p \rightarrow (f_1(p), \cdots, f_d(p))$$

of U into E^d and let f_0 be the restriction of f to P. Let λ and ω respectively be the multiplicity and multiplicity function, as defined in Theorem 2, of the map f_0 of P into E^d. Consider p_0 in $U - L$ and write $z_0 = f(p_0)$. Since K is a Stein manifold there exists w in $A(K)$ such that $w(p_0) \neq w(p)$ for all p in $\omega(z_0)$.

For an arbitrary point q in U let $\omega(f(q)) = \{q_1, \cdots, q_\lambda\}$. Define the function h on U by

$$(*) \qquad h(q) = \prod_{i=1}^{\lambda} (w(q) - w(q_i)).$$

Thus h is a polynomial in w whose coefficients a_j, $0 \leqq j \leqq \lambda$, are symmetric functions of the q_i. Clearly a_j is a continuous function on P which is analytic on L at each point of the set J defined in Theorem 3. By Theorem 3 the functions a_j are analytic on U. It follows that h is analytic on U. Clearly $h(p_0) \neq 0$ and h vanishes on $L \cap U \subset P$. This proves I_1.

To prove II_1, define $f_1, \cdots, f_k$ and P as above. Choose r_0 with $0 < r_0 < 1$ such that $|f_i(p)| < r_0$, $1 \leqq i \leqq d$, $p \in \bar{U}$. Choose a real number r with $r_0 < r < 1$. Write

$$T = \{p \in P : |f_i(p)| \leqq r, 1 \leqq i \leqq d\}$$

whenever $0 < r < 1$. Let p_0 be any point of T. Since K is a Stein manifold there exist $h_1, \cdots, h_d$ in $A(K)$ whose restrictions to L are a coordinate set of functions on L at the point p_0. Thus for all sufficiently small $\epsilon \neq 0$ the functions

$$g_i = f_i + \epsilon h_i \qquad 1 \leqq i \leqq d$$

are a coordinate set of functions on L at the point p_0. It follows from the choice of r_0 that $|g_i(p)| < r_0$, $1 \leqq i \leqq d$, for all p in $\bar{U}$ if ϵ is small enough. Now fix r_1 with $r < r_1 < 1$. Consider the sets

$$R_0 = \{p \in P : |g_i(p)| < r_0, 1 \leqq i \leqq d\}$$

and

$$R_1 = \{p \in P : |g_i(p)| < r_1, 1 \leqq i \leqq d\}.$$

If ϵ is small enough then R_0 and R_1 are analytic polyhedra in L defined by multiples of the functions $g_1, \cdots, g_d$ with $R_0 \subset T \subset R_1 \subset P$. Let g be the map $(g_1, \cdots, g_d)$ of K into C^d and let $\tilde{g}$ be the restriction of g to R_1. From Theorem 2 it follows that the map $\tilde{g}$ of R_1 into $r_1 E^d$ has a definite multiplicity

λ and multiplicity function ω. Since $g_1, \cdots, g_d$ form a coordinate system at p_0, the point p_0 occurs with multiplicity 1 in the set $\omega(g(p_0))$. Let w be any function in $A(K)$ whose value at p_0 is different from its values at the other points of $\omega(g(p_0))$.

For an arbitrary q in $g^{-1}(r_1 E^d)$ let $q_1, \cdots, q_\lambda$ be the points of the set $\omega(g(q)) = \{q_1, \cdots, q_\lambda\}$, counted according to multiplicity. Let u be any function analytic on R_0. Define the function $\tilde{u}$ on $g^{-1}(r_0 E^d) \supset U$ by

$$\text{(a)} \qquad \tilde{u}(q) = \sum_{i=1}^{\lambda} [u(q_i) \prod_{j \neq i} (w(q) - w(q_j))].$$

Now $\tilde{u}(q)$ is a polynomial in $w(q)$ whose coefficients $a_0(q), \cdots, a_\lambda(q)$ are analytic functions of q at each point q in $g^{-1}(r_0 E^d)$ for which $q_1, \cdots, q_\lambda$ are disinct points of R_0. By Theorem 3, the functions a_i are analytic on U. Therefore $\tilde{u}$ is analytic on U. For q in $U \cap L \subset R_0$ the point q is one of the points $q_1, \cdots, q_\lambda$ in $\omega(g(q))$, say $q = q_1$. In this case it is clear that

$$\text{(b)} \qquad \tilde{u}(q) = u(q) \tilde{w}(q)$$

where

$$\text{(c)} \qquad \tilde{w}(q) = \prod_{i=2}^{\lambda} (w(q) - w(q_i))$$

is an analytic function on R_1, it being understood that q_1 is chosen to equal q for q in R_1. Remembering that p_0 occurs with multiplicity 1 in the set $\omega(g(p_0))$ and that w takes on values other than $w(p_0)$ at the other points of $\omega(g(p_0))$, we see that $\tilde{w}(p_0) \neq 0$.

Thus for each p_0 in T there exists a function $\tilde{w}$ analytic on R_1 with $\tilde{w}(p_0) \neq 0$ such that for every analytic function u on R_0 there exists an analytic function $\tilde{u}$ on U which agrees with $u\tilde{w}$ on $U \cap L$. Let B be the uniform closure on T of all functions analytic on R_1. From Theorem 4 we see that the spectrum of B is T. Since the function $\tilde{w}$, which is analytic on R_1, can be chosen to be non-zero at any given point of T, there exist a finite number $\tilde{w}_1, \cdots, \tilde{w}_N$ of such functions which have no common zero in T. Thus from the general theory of Banach algebras there exist elements $c_1, \cdots, c_N$ of B with

$$\text{(d)} \qquad c_1 \tilde{w}_1 + \cdots + c_N \tilde{w}_N = 1.$$

For each j, $1 \leqq j \leqq N$, let $\tilde{u}_j$ be the function defined by (a) with w replaced by w_j and u replaced by $c_j u$. Thus

$$\text{(e)} \qquad \bar{u} = \sum_{j=1}^{N} \tilde{u}_j$$

is analytic on U, and for all q in $U \cap L$ we have, by (b), (d), and (e)

$$\begin{aligned}\bar{u}(q) &= \sum \tilde{u}_j(q) = \sum c_j(q) u(q) \tilde{w}_j(q)\\ &= [\sum c_j(q) \tilde{w}_j(q)] u(q) = u(q).\end{aligned}$$

This completes the proof of II_1.

Remark. Theorem II_1 holds in the following greater generality. Let V be a complex vector space and W some set of linear functionals on V. Define a function u with values in V to be analytic if $\phi \circ u$ is analytic for all ϕ in W. Then Theorem II_1 holds for analytic functions with values in V.

We now prove I and II.

THEOREM 8. *Let L be an analytic subset of a Stein manifold K. Let L have dimension d at each of its points. Then*

- I. *For each p_0 in $K - L$ there exists an analytic function h on K, defined by (*) and (‡) below, which vanishes on L but does not vanish at p_0.*
- II. *If L is a submanifold of K then corresponding to every analytic function u on L there exists an analytic function $\bar{u}$ on K with $\bar{u}(q) = u(q)$ for all q in L. The function $\bar{u}$ is given by a conglomeration of formulas which are summarized by * below.*

Proof. By Theorem 5, there exists an analytic map $f = (f_1, \cdots, f_d)$ of K into C^d whose restriction $\bar{f}$ to L is almost proper. If $p \in K$ then $\bar{f}^{-1}(f(p))$ is countable and consists of isolated points. Let $p_1, \cdots, p_n, \cdots$ be the points of $\bar{f}^{-1}(f(p))$, each being counted a number of times equal to its multiplicity for the mapping $\bar{f}$. The multiplicity of a point q for the mapping $\bar{f}$ is defined by considering a special analytic polyhedron Q in L containing q defined by multiples of $f_1, \cdots, f_d$ and taking the multiplicity of q for the analytic polyhedron Q; this multiplicity does not depend on the choice of Q.

Let $\{S_k\}$ be a sequence of compact subsets of L, each of which has finitely many components, with $S_k \subset S_{k+1}$ for all k and $\cup_k \operatorname{int} S_k = L$. For each positive integer k let H_k be the union of those components of $\bar{f}^{-1}(\alpha(k) \bar{E}^d)$ which intersect S_k, where $\alpha(k) > k + 1$ is chosen so that $f(S_k) \subset \alpha(k) E^d$. Thus $S_k \subset H_k$. Write

$$G_k = (\bar{f}^{-1}(\alpha(k) \bar{E}^d) \cap H_{k+1}) - H_k$$

for all positive integers k. Now $\operatorname{int} H_k = H_k \cap \bar{f}^{-1}(\alpha(k) E^d)$ is an analytic polyhedron defined by the functions $\alpha(k)^{-1} f_1, \cdots, \alpha(k)^{-1} f_d$. Let λ_k be the multiplicity of $\operatorname{int} H_k$. Thus for each p in K the number of points in the sequence $p_1, p_2, \cdots$ belonging to $\operatorname{int} H_k$ is either λ_k or 0, depending on whether $f(p)$ is in $\alpha(k)E^d$ or not. By Theorem 6, there exists f_{d+1} in $A(K)$ such that

$$|f_{d+1}(p) - (\lambda_{k+1} + k^2 + 1)| < 1$$

for all p in G_k and all k. Therefore

$$\mathfrak{R}(f_{d+1}(p)) \geqq \lambda_{k+1} + k^2$$

for all p in G_k. If p_0 is any point in $K - L$, we may choose f_{d+1} so that in addition

$$\exp(f_{d+1}(p_0)) \neq \exp(f_{d+1}(q))$$

for all q in $f^{-1}(f(p_0))$. Write

$$w = \exp(-f_{d+1})$$

so that $w \in A(K)$ and

$$|w(p)| \leqq \exp(-\lambda_{k+1} - k^2) \leqq (k^2\lambda_{k+1})^{-1}$$

for all p in G_k. Choose $k_0 \geqq 2$ with $f(T) \subset k_0E^d$, where T is a compact subset of K to be fixed later. Since $\{H_k\}$ is an increasing sequence of sets whose union is K, there exists for each q in $f^{-1}(f(T))$ a smallest k with $q \in H_k$. If $k > k_0$ then $q \in G_{k-1}$; in fact, $q \in \operatorname{int} G_{k-1}$ because $f(q) \in k_0E^d \subset kE^d$ so that $q \in f^{-1}(kE^d) \cap G_{k-1} \subset \operatorname{int} G_{k-1}$. If $k = k_0$ then similarly $q \in \operatorname{int} H_{k_0}$. Thus

$$f^{-1}(f(T)) \subset \operatorname{int} H_{k_0} \cup \bigcup_{k=k_0}^{\infty} \operatorname{int} G_k.$$

Now for each p in K and $k \geqq 1$ define

$$(*) \qquad h_k(p) = \prod (1 - w(p_i)[w(p)]^{-1}),$$

where the product is taken over all p_i in F_k, with $F_1 = H_1$ and $F_k = H_k - H_{k-1}$ for $k > 1$. Since at most λ_k of the p_i belong to H_k and since w does not vanish on K, we see that the functions h_k are well-defined. We shall show that the product

$$(⁑) \qquad h(p) = \prod_{k=1}^{\infty} h_k(p)$$

converges uniformly on all compact subsets of K and defines a function h in $A(K)$. Assuming for the moment that this is so, it follows from the fact that $p = p_i$ for some i whenever $p \in L$ that h vanishes on L. It follows from the fact that w has values none of which equal $w(p_0)$ at the points of $f^{-1}(f(p_0))$ that $h(p_0) \neq 0$. Thus h has all of the desired properties. It remains to prove the convergence of the product (‡) to a function h in $A(K)$. For this purpose it is sufficient to consider an open subset U of K whose closure T is compact. Fix T to be the compact set considered above. Write

$$h_0(p) = \prod(1 - w(p_i)[w(p)]^{-1}),$$

where the product is taken over all p_i in $\operatorname{int} H_{k_0}$. Thus by the above we see that for all p in T

$$h_0(p) = \prod_{k=1}^{k_0} h_k(p).$$

Similarly

$$h_k(p) = \prod(1 - w(p_i)[w(p)]^{-1})$$

for all p in T and $k \geqq k_0$, where the product is taken over all p_i in $\operatorname{int} G_k$. Now for $k \geqq k_0$, h_k is a polynomial in $[w(p)]^{-1}$ whose coefficients we denote by $a_j(p)$. Clearly a_j is an analytic function of p for all p for which the points p_i in G_k are distinct. Since $\operatorname{int} G_k$ is an analytic polyhedron defined by a multiple of the functions $f_1, \cdots, f_d$, it follows from Theorem 3 that h_k is analytic on $f^{-1}(f(\operatorname{int} G_k)) \supset U$. Similarly h_0 is analytic on U. Thus we need only check the uniform convergence of the product

$$\prod_{k=k_0}^{\infty} h_k$$

on U. To do this we may equally well consider the series

$$\sum_{k=k_0}^{\infty} (\Sigma\{p_i \text{ in } G_k : |w(p_i)|\}),$$

since $|w|$ is bounded below on the compact set T. The sum over p_i in G_k contains at most λ_{k+1} terms, each bounded by $(k^2\lambda_{k+1})^{-1}$, and so is at most k^{-2}. Thus the series converges absolutely and uniformly on T. This completes the proof of I.

We turn to the proof of II. Define $\{S_k\}$, $f_1, \cdots, f_d$, $\bar{f}$, G_k, H_k, T, p_1, $p_2, \cdots, \lambda_k$, f_{d+1}, and w as above. For p in L choose $p_1 = p$. In addition choose $f_1, \cdots, f_d$ to be a coordinate system on L at $\bar{p}$ for all $\bar{p}$ in a given 0-dimensional subset of L. Also choose w to have distinct values at the points of $\bar{f}^{-1}(f(\bar{p}))$. For each positive integer k define the function h_k on K by

$$h_k(p) = \sum u(p_i)c(p_i)d(p_i)[\prod_{j \neq i}(1 - w(p_j)[w(p)]^{-1})]$$

where the product and sum are taken over points p_i and p_j in H_k. Here c is a given function in $A(L)$ and d is a function in $A(K)$ which will be determined later. Let $U \subset K$ have compact closure T. Consider k so large that $f(T) \subset a(k)E^d$. Now if $f(p) \in a(k)E^d$ then $f(p_i) = f(p) \in a(k)E^d$ for all i. Thus we see that $p_i \in \operatorname{int} H_k$ whenever $f(p) \in a(k)E^d$ and $p_i \in H_k$. From this it is clear that each of the coefficients $a_j(p)$ in the expansion of $h_k(p)$ in powers of $[w(p)]^{-1}$ defines a continuous function a_j on $f^{-1}(a(k)E^d)$ which is analytic at every point p of $f^{-1}(a(k)E^d)$ which has the property that the points p_i which lie in H_k are distinct. By Theorem 3, a_j is analytic on $U \subset f^{-1}(a(k)E^d)$. Thus h_k is analytic on U for all k sufficiently large. If $j > k$ then

$$|h_j(p) - h_k(p)| \leqq AB + CD(E-1),$$

where A is the sum

$$\Sigma = \Sigma \, |u(p_i)| \, |c(p_i)| \, |d(p_i)|$$

taken over p_i in $L - H_k$, B is the product

$$\Pi = \Pi(1 + |w(p_i)| \, |w(p)|^{-1})$$

taken over all p_i, C is the sum $\sum$ taken over p_i in H_k, D is the product $\prod$ taken over p_i in H_k and E is the product $\prod$ taken over p_i in $L - H_k$. Thus to show uniform convergence of the sequence $\{h_k\}$ on the set U we must show that the terms AB and $CD(E-1)$ converge to 0 as $k \to \infty$. We consider only the term AB, since the treatment of the other term is entirely similar. Now the product B is finite and bounded independently of p if $p \in U$, as may be seen by considering the sum

$$\sum_{j=1}^{\infty} |w(p_j)|,$$

where the factors $|w(p)|^{-1}$ have been left out because $|w|$ is bounded independently of p in U. Thus to show that the sequence $\{h_k\}$ converges uniformly to 0 on U as $k \to \infty$ we need only show that $A \to 0$ uniformly on U as $k \to \infty$. This will be done by an appropriate choice of the function d. Let

$$\beta_k = \sup\{|u(p)c(p)| : p \in G_k\}.$$

By Theorem 5 there exists f'_{d+1} in $A(K)$ such that

$$|f'_{d+1}(p) - k^2\beta_k\lambda_{k+1} - 1| < 1$$

for all p in G_k, so that $\mathfrak{R}(f'_{d+1}(p)) \geqq k^2\beta_k\lambda_{k+1}$. Let $d = \exp(-f'_{d+1})$, so that $d \in A(K)$ and d vanishes nowhere on K. Also

$$|d(p)| < (k^2\beta_k\lambda_{k+1})^{-1}$$

for all p in G_k. Now if $p \in U$ and k_0 is chosen so large that $f(T) \subset k_0E^d$

each p_i in $L - H_{k_0}$ is in some G_k for $k > k_0$. Therefore the sum A splits into partial sums A_k taken over the sets G_k for $k \geqq k_0$. Now at most λ_{k+1} of the points p_i lie in G_k. It follows from the choice of d that

$$A_k \leqq (k^2\beta_k\lambda_{k+1})^{-1}\beta_k\lambda_{k+1} = k^{-2}.$$

Thus $A \leqq \sum_{k=k_0}^{\infty} k^{-2}$. Hence $\{h_k\}$ converges uniformly on U. It follows that $\{h_k\}$ converges uniformly on compact subsets of K to a function $\tilde{u}$ in $A(K)$. For p in L we have, remembering that in this case p_1 is chosen to be p,

$$h_k(p) = u(p)c(p)d(p)\prod_{j\neq 1}(1 - w(p_j)[w(p)]^{-1}),$$

where the product is taken over all p_j in H_k. Thus, passing to the limit,

$$\tilde{u}(p) = u(p)c(p)d(p)\tilde{w}(p),$$

where

$$w(p) = \prod_{j=2}^{\infty}(1 - w(p_j)[w(p)]^{-1}).$$

By the choice of $f_1, \cdots, f_d$, $p_j \neq p$ for $j \geqq 2$ if $p = \bar{p}$. By the choice of w it follows that $\tilde{w}(\bar{p}) \neq 0$.

We have thus found a function $\tilde{w} = \tilde{w}_1$ on L such that for any c_1 in $A(L)$ there exists d_1 in $A(K)$ vanishing nowhere such that there is a function $\tilde{u}_1$ in $A(K)$ which equals $uc_1d_1\tilde{w}_1$ on L. We may choose $\tilde{w}_1$ not to vanish at a 0-dimensional subset of L which contains points in each component of L. Thus the set L_1 of zeros of $\tilde{w}_1$ is of dimension at most $d - 1$. Now choose $\tilde{w}_2$ to have the same properties as $\tilde{w}_1$ and to be non zero at a 0-dimensional subset of L_1 containing points in each analytic component of L_1. Continuing in this fashion we find $\tilde{w}_1, \cdots, \tilde{w}_d$ having the above properties and having no common zero on L. By a theorem of Arens [1] [2] it follows that there exist $c_1, \cdots, c_d$ in $A(L)$ with

$$\sum c_i\tilde{w}_i = 1.$$

By the choice of w_i, there exists d_i in $A(K)$ vanishing nowhere on $A(K)$ such that $uc_id_i\tilde{w}_i$ has an extension from L to an analytic function $\tilde{u}_i$ on K. Write

$$\tilde{u} = \sum_{i=1}^{d}(d_i)^{-1}\tilde{u}_1,$$

---

[2] The possibility of using Arens' theorem here was pointed out by Kenneth Hoffman.

so that $\tilde{u} \in A(K)$. For p in L we have

$$\tilde{u}(p) = \sum_{i=1}^{d} (d_i(p))^{-1} u(p) c_i(p) d_i(p) \tilde{w}_i(p)$$
$$= u(p) \sum_{i=1}^{d} c_i(p) \tilde{w}_i(p) = u(p).$$

This completes the proof of II. The final formula reads

$$* \quad \tilde{u}(p) = \sum_{n=1}^{d} (d_n(p))^{-1} \sum_{i=1}^{\infty} u(p_i) c_n(p_i) d_n(p_i) [\prod_{j \neq i} (1 - w_n(p_j)[w_n(p)]^{-1})].$$

Remark. As is well-known, II (in fact II_1) can be used to prove Runge's theorem for Stein manifolds. The proof goes as follows. Let T be a compact subset of a Stein manifold K and h a function analytic in some neighborhood U of T. Runge's theorem says that h can be uniformly approximated on T by functions in $A(K)$ if for each p in $U - T$ there exists in $A(K)$ with $|g(p)| > \max\{|g(q)| : q \in T\}$. To show this notice that the assumption implies that there exists an analytic polyhedron P in K with

$$T \subset P \subset U.$$

Let $f_1, \cdots, f_k$ be the functions defining P. Choose $f_{k+1}, \cdots, f_n$ in $A(K)$ to separate points of U and to have rank equal to the dimension of K at each point of U. We may assume that $|f_i(p)| < 1$ for all p in T, $k + 1 \leqq i \leqq n$. Thus the map $f = (f_1, \cdots, f_n)$ of K into C^n maps T into E^n. Also $M = f(P)$ is a submanifold of E^n. Let $\hat{f}$ be the analytic homeomorphism of M onto P which is inverse to f, and let u be the analytic function $h \circ \hat{f}$ on L. By II, u admits an analytic extension $\tilde{u}$ to E^n. By a well-known and elementary use of the Cauchy integral formula, $\tilde{u}$ can be uniformly approximated on $f(T)$ by functions v analytic on E^n. Thus the functions $v \circ f$ in $A(K)$ uniformly approximate h on T, as was desired.

4. The resolution of Cousin distributions.

As is well-known, the solution on a Stein manifold of Cousin's first problem, which consists of the global construction of a meromorphic function whose principal parts are locally given, can be obtained from the fact that on a Stein manifold the sheaf of germs of analytic functions has a first cohomology group which is trivial. Cousin's second problem, which states that a globally defined meromorphic function exists whose quotients with certain locally given meromorphic functions are analytic functions without zeros, can also be solved using this statement about cohomology. Thus we shall restrict ourselves in this section to showing that the cohomology group in question is trivial. This will be done without the use of cohomological terminology.

Definition 5. Let U be an open subset of a Stein manifold K. A *Cousin distribution* on U will consist of a covering $\{U_\alpha\}$ of U by open sets and an assignment for each α and β of an analytic function $f_{\alpha\beta}$ to the intersection $U_\alpha \cap U_\beta$ such that

(a) $$f_{\alpha\beta} + f_{\beta\alpha} = 0$$

and

(b) $$f_{\alpha\beta} + f_{\beta\gamma} + f_{\gamma\alpha} = 0 \qquad \text{on } U_\alpha \cap U_\beta \cap U_\gamma.$$

for all α, β, and γ. By a *resolution* of the given distribution $\{U_\alpha\}$, $\{f_{\alpha\beta}\}$ on an open set $S \subset K$ we mean a family $\{f_\alpha\}$, where f_α is analytic on $S \cap U_\alpha$, such that

$$f_{\alpha\beta} = f_\alpha - f_\beta \qquad \text{on } S \cap U_\alpha \cap U$$

for all α and β.

By a *refinement* of the distribution $\{U_\alpha\}$, $\{f_{\alpha\beta}\}$ we mean a Cousin distribution $\{V_\gamma\}$, $\{g_{\gamma\delta}\}$ and a mapping σ of the index set of $\{V_\gamma\}$ into the index set of $\{U_\alpha\}$ such that

(c) $$V_\gamma \subset U_{\sigma(\gamma)}$$

and

(d) $$g_{\gamma\delta} = f_{\sigma(\gamma)\sigma(\delta)} \qquad \text{on } V_\gamma \cap V_\delta$$

for all γ and δ. If T is a compact subset of K then a Cousin distribution on T means a Cousin distribution on some neighborhood U of T, and a resolution on T means a resolution on some neighborhood of T. The same definitions will be taken to hold if the functions $f_{\alpha\beta}$ etcetera are replaced by polynomials of given degree in an indeterminate X whose coefficients are analytic functions on the appropriate sets.

We make use below of the trivial fact that a Cousin distribution which has a refinement with a resolution itself has a resolution.

The cohomology theorem mentioned above is just the statement that every set of Cousin data on a Stein manifold K has a resolution on K, and it is this fact which will be proved below. As a tool we shall use the fact that every Cousin distribution on the subset E^n of C^n has a resolution. This is well-known to be a completely elementary fact and indeed was essentially proved by Cousin [4]. For completeness however we sketch the proof at the end of this section. The following lemma contains the essence of the theorem to be proved.

Lemma 1. *Let T be a compact set of a Stein manifold K and Δ a neighborhood of T such that for all p in $\Delta - T$ there exists f in $A(K)$ with*

$$f(p) > \sup\{|f(q)| : q \in T\}.$$

Then any Cousin distribution on T has a resolution on the interior M of T.

Proof. Let the given Cousin data $\{U_\alpha\}$, $\{f_{\alpha\beta}\}$ be defined on an open set $U \supset T$. Let P be a special analytic polyhedron defined by functions $f_1, \cdots, f_d$ in $A(K)$ with $T \subset P \subset \bar{P} \subset U$. Choose a covering $\{V_\gamma\}$ of E^d so fine that each component of $W_\gamma = P \cap f^{-1}(V_\gamma)$ lies in one of the sets U_α for each γ. Since P is a special analytic polyhedron, each W_γ has only a finite number of components, which we denote by $W_1{}^\gamma, \cdots, W_t{}^\gamma$, where t depends on γ. For each of these components $W_i{}^\gamma$ choose $U_{\alpha(i\gamma)}$ in $\{U_\alpha\}$ with $W_i{}^\gamma \subset U_{\alpha(i\gamma)}$. For each γ and δ define the analytic function $h_{\gamma\delta}$ on $W_\gamma \cap W_\delta$ by

$$h_{\gamma\delta}(p) = f_{\alpha(i\gamma)\alpha(j\delta)}$$

for all p in $W_i{}^\gamma \cap W_j{}^\delta$. It is easy to see that $\{W_\gamma\}$, $\{h_{\gamma\delta}\}$ is a Cousin distribution on P. For each point z in E^d let $p_1, \cdots, p_\lambda$ be the points of $\omega(z) = \{p_1, \cdots, p_\lambda\}$. Let w be any function in $A(K)$. Let X be an indeterminate. For each γ and δ and each z in $V_\gamma \cap V_\delta$ define

$$g_{\gamma\delta}(z, X) = \sum_{j=1}^{\lambda} h_{\gamma\delta}(p_i) \prod_{j \neq i} (X - w(p_j)).$$

By Theorem 3 we see that the coefficient of each power of X in the polynomial $g_{\gamma\delta}$ in X is analytic on $V_\gamma \cap V_\delta$. Since $\{W_\gamma\}$, $\{h_{\gamma\delta}\}$ is a Cousin distribution on P we see that

$$g_{\gamma\delta} + g_{\delta\gamma} = 0$$

and

$$g_{\gamma\delta} + g_{\gamma\sigma} + g_{\sigma\gamma} = 0$$

for all γ, δ, and σ. Thus $\{V_\gamma\}$, $\{g_{\gamma\delta}\}$ is a Cousin distribution for E^d. By the statement made above (whose proof will be outlined below), there exists a resolution $\{g_\gamma\}$ of this Cousin distribution. Now $\{W_i{}^\gamma\}$ is a covering of P. For each $W_i{}^\gamma$ define the function $F_{i\gamma}$ an $W_i{}^\gamma$ by

$$F_{i\gamma}(p) = g_\gamma(f(p), w(p)).$$

These functions are the resolution of a Cousin distribution $\{W_i{}^\gamma\}$, $\{F_{i\gamma j\delta}\}$ on P, where $F_{i\gamma j\delta}$ is the function

$$F_{i\gamma}(p) - F_{j\delta}(p) = g_{\gamma\delta}(f(p), w(p))$$

on $W_i^\gamma \cap W_j^\delta$. If for each p in P we write $\omega(f(p)) = \{p_1, \cdots, p_\lambda\}$, with $p_1 = p$, it follows that

$$\begin{aligned} F_{i\gamma j\delta}(p) &= \sum_{i=1}^{\lambda} h_{\gamma\delta}(p_i) \prod_{j \neq i} (w(p) - w(p_j)) \\ &= h_{\gamma\delta}(p) \prod_{i=2}^{\lambda} (w(p) - w(p_j)) \\ &= \tilde{w}(p) h_{\gamma\delta}(p) = \tilde{w}(p) f_{\alpha(i\gamma)\alpha(j\delta)}(p), \end{aligned}$$

where $\tilde{w}$ is the analytic function on P defined by

$$\tilde{w}(p) = \prod_{j=2}^{\lambda} (w(p) - w(p_j)).$$

Thus $\{F_{i\gamma j\delta}\}$ is a resolution on P, and therefore on M, of the distribution $\{W_i^\gamma\}$, $\{\tilde{w} f_{\alpha(i\gamma)\alpha(j\delta)}\}$. Since this distribution is a refinement on M of the distribution $\{U_\alpha\}$, $\{\tilde{w} f_{\alpha\beta}\}$, it follows that the latter distribution has a resolution on M.

If p_0 is any point in T we may assume that $f_1, \cdots, f_d$ were chosen so that f has multiplicity 1 at p_0 and that w was chosen to distinguish p_0 from the other points of $\omega(f(p_0))$, so that $\tilde{w}(p_0) \neq 0$. Thus we can find a finite number of functions $\tilde{w}_1, \cdots, \tilde{w}_n$, each analytic in some neighborhood of T and having no common zero on T, such that for $1 \leqq i \leqq n$ the distribution $\{U_\alpha\}$, $\{\tilde{w}_i f_{\alpha\beta}\}$ has a resolution on M. Thus for each c_i analytic on M the distribution $\{U_\alpha\}$, $\{\tilde{w}_i c_i f_{\alpha\beta}\}$ has a resolution on M. By Theorem 4, the c_i may be chosen ith $\sum c_i \tilde{w}_i = 1$. It follows that distribution $\{U_\alpha\}$, $\{f_{\alpha\beta}\}$, which on M is therefore the sum of distributions which have resolutions on M, has a resolution on M. This completes the proof.

THEOREM 9. *Any Cousin distribution on a Stein manifold K has a resolution on K.*

Proof. Since K is Stein, there exists an increasing sequence $\{M_n\}$ of open sets whose union is K and whose closures T_n all have the property of the set T of Lemma 1. Thus for each n by Lemma 1 the given Cousin distribution $\{U_\alpha\}$, $\{f_{\alpha\beta}\}$ has a resolution $\{f_\alpha{}^n\}$ on M_n. We may assume that the closure of each U_α is compact. Let $\{S_n\}$ be an increasing sequence of compact sets whose union is K, which have the property of the set T in Lemma 1, and which satisfy the inclusion $S_n \subset M_n$. We show now by induction on n that for each n there exists a resolution $\{h_\alpha{}^n\}$ of $\{U_\alpha\}$, $\{f_{\alpha\beta}\}$ on M_n such that

$$|h_\alpha{}^{n-1}(p) - h_\alpha{}^n(p)| < 2^{-n}$$

for all p in S_{n-1}. Assume that the $h_\alpha{}^n$ have been found for all integers smaller than a given integer n. For each p in M_{n-1} choose α with p in U_α and write

$$g_0(p) = h_\alpha^{n-1}(p) - f_\alpha^n(p).$$

It is easily seen that g_0 is an analytic function on M_{n-1}. By Runge's Theorem there exists g in $A(K)$ with

$$|g(p) - g_0(p)| < 2^{-n}$$

for all p in S_{n-1}. It follows that the functions $\{h_\alpha^n\}$ have the required properties, where $h_\alpha^n = f_\alpha^n + g$ on $U_\alpha \cap M_n$. Since the closure of each U_α is compact, it follows that for each fixed α the sequence $\{h_\alpha^n\}$ converges uniformly on U_α to a function $\{f_\alpha\}$. These functions clearly form a resolution on K of the given Cousin distribution. This completes the proof.

Remark. If a meromorphic function with values in a Banach space is defined to be one which is locally a quotient of an analytic Banach-space valued function by an analytic scalar-valued function, then Cousin's first and second problems can be solved for such functions by applying Theorem 9 for Banach-space valued Cousin distributions.

To finish we indicate the technique for obtaning a resolution of a Cousin distribution on E. Let D be the set

$$\{(z_1, \cdots, z_d) \in C^d \colon z = x_n + iy_n, |x_n| < 1, |y_n| < 1, 1 \leqq n \leqq d\}.$$

Since D^d is conformally equivalent to E^d, we may equally well consider the resolution of a Cousin distribution given on D^d. In fact we may assume that the distribution is given on the closure H^d of D^d, as the proof of Theorem 9 shows. Let the given distribution be $\{U_\alpha\}$, $\{f_{\alpha\beta}\}$, given on H^d. We first introduce the notion of a *soft resolution* for a Cousin distribution. This is the same as a resolution except that the functions f_α are permitted to be the arbitrary (not necessarily analytic) functions. It is easy to see that every Cousin distribution has a soft resolution. Let $\{F\}_\alpha$ be a soft resolution of the given distribution. If U is an open set then it is easy to check that the given distribution has a resolution on U if and only if there exist a function F on U such that $F - F_\alpha$ is analytic on $U_\alpha \cap U$ for all α. Let $z_n = x_n + iy_n$, $1 \leqq n \leqq d$, be the coordinates in C^d. Let N be a positive integer and write

$$S_n(k) = \{z \in H^d \colon -1 + \frac{k-1}{N} \leqq x_n \leqq -1 + \frac{k}{N}\}$$

for $1 \leqq k \leqq 2N$ and $1 \leqq n \leqq 2d$. For each choice of $k_1, \cdots, k_{2d}$, with $1 \leqq k_j \leqq 2N$, write

$$S(k_1, \cdots, k_{2d}) = S_1(k_1) \cap \cdots \cap S_{2d}(k_{2d}).$$

Choose N so large that the covering $\{S(k_1,\cdots,k_{2d})\}$ of H^d is a refinement of the covering $\{U_\alpha\}$ of H^d. For each $k_1,\cdots,k_t$, with $1 \leqq k_j \leqq 2N$ and $0 \leqq t \leqq 2d$, let

$$S(k_1,\cdots,k_t) = S_1(k_1) \cap \cdots \cap S_t(k_t)$$

so that $S(\emptyset) = H^d$. We shall show that the given Cousin distribution has a resolution on each $S(k_1,\cdots,k_t)$. This is true if $t = 2d$ because the covering $\{S(k_1,\cdots,k_{2d})\}$ is a refinement of $\{U_\alpha\}$. Assume therefore that it is true for all t greater than some given t, so that we must show that there is a resolution on each $S(k_1,\cdots,k_t)$. To this end write for each $1 \leqq k \leqq 2N$

$$S(k_1,\cdots,k_t;k) = S(k_1,\cdots,k_t) \cap \bigcup_{j=1}^{k} S_{t+1}(j) = \bigcup_{j=1}^{k} S(k_1,\cdots,k_t,j)$$

Thus

$$S(k_1,\cdots,k_t;k+1) = S(k_1,\cdots,k_t;k) \cup S(k_1,\cdots,k_t,k+1)$$

and

$$S(k_1,\cdots,k_t;1) = S(k_1,\cdots,k_t,1).$$

By the induction hypothesis on t, it follows that the given distribution has a resolution on $S(k_1,\cdots,k_t;1)$. We now show by induction on k (t remaining fixed) that the given distribution has a resolution on $S(k_1,\cdots,k_t;k)$. Assume therefore that this is true for all k smaller than the given k. Thus by the above we see that there exists a neighborhood V_1 of $S(k_1,\cdots,k_t;k-1)$ and a function G_1 on V_1 such that $G_1 - F_\alpha$ is analytic on $V_1 \cap U_\alpha$ for all α. Similarly, there exists a function G_0 on some neighborhood V_2 of $S(k_1,\cdots,k_t,k)$ such that $G_2 - F_\alpha$ is analytic on $V_2 \cap U_\alpha$ for all α. Thus $G_1 - G_2$ is analytic on $V_1 \cap V_2$. It is well known and easy to see that therefore there exist open sets W_1 and W_2 with

$$S(k_1,\cdots,k_t;k-1) \subset W_1 \subset V_1$$

and

$$S(k_1,\cdots,k_t,k) \subset W_2 \subset V_2$$

and analytic functions A_1 and A_2 on W_1 and W_2 respectively such that $A_2 - A_1$ and $G_1 - G_2$ are equal on $W_1 \cap W_2$. It follows that the function B on $W_1 \cup W_2$ defined as $A_1 + G_1$ on W_1 and $A_2 + G_2$ on W_2 has the property that $B - F_\alpha$ is analytic on $(W_1 \cup W_2) \cap U_\alpha$ for all α. Thus the given distribution has a resolution on

$$S(k_1,\cdots,k_t;k) = S(k_1,\cdots,k_t;k-1) \cup S(k_1,\cdots,k_t,k) \subset W_1 \cup W_2.$$

This completes the induction on k. It follows that there exists a resolution on

$$S(k_1,\cdots,k_t;2N) = S(k_1,\cdots,k_t).$$

This in turn completes the induction on t. It follows that there exists a resolution on $S(\emptyset) = H^d$, as was to be proved.

Added in proof: Let L be an analytic submanifod of dimension d in a Stein manifold K. Let U be an open relatively compact subset of K. Then the contruction used in the proof of Theorem II_1 shows that there exists a multiple-valued projection of U into L in the following sense. There exists an integer λ and an analytic map

$$p \to \{(p_1, z_1), \cdots, (p_\lambda, z_\lambda)\}$$

of U into the λ-fold unordered product ${}_\lambda\Omega$ of the space $\Omega = L \times C$ with itself having the following properties. For each p in U,

$$z_1 + \cdots + z_\lambda = 1.$$

For each p in $L \cap U$ and each i with $1 \leqq i \leqq \lambda$ for which $p_i \neq p$ we have $z_i = 0$. This fact in turn clearly implies Theorem II_1, since u can be extended from L to U by the formula

$$u(p) = \sum_{i=1}^{\lambda} z_i u(p_i).$$

Similarly the proof of Theorem II can be used to show the existence of certain multiple-valued analytic projections of K into L.

UNIVERSITY OF CALIFORNIA, BERKELEY.

REFERENCES.

[1] Richard Arens, "Dense inverse limit rings," *Michigan Mathematical Journal*, vol. 5 (1958), pp. 169-182.

[2] Errett Bishop, "Mappings of partially analytic spaces," *American Journal of Mathematics*, vol. 83 (1961), pp. 209-242.

[3] Henri Cartan, "Seminaire E. N. S.," 1951-52.

[4] P. Cousin, "Sur les fonctions de *n* variables complexes," *Acta Mathematica*, vol. 19 (1895).

[5] Kiyosi Oka, "Sur les fonctions analytiques de plusieurs variables. I-Domaines convexes par rapport aux fonctions rationelles," *Journal of Science of Hiroshima University*, vol. 6 (1936), pp. 245-255.

[6] ———, "Sur les fonctions analytiques de plusieurs variables. II-Domaines d'holomorphie," *Journal of Science of Hihoshima University*, vol. 7 (1937), pp. 115-130.

[7] ———, "Sur les fonctions analytiques de plusieurs variables. III-Deuxième problème de Cousin," *Journal of Science of Hiroshima University*, vol. 9 (1939), pp. 7-19.

ON INDUCED REPRESENTATIONS II: INFINITESIMAL INDUCTION.*

By ROBERT J. BLATTNER.[1]

---

1. Introduction. This paper is a continuation of the investigation begun in [1].[2] We take as our point of departure some observation of Gelfand and Graev in [3] concerning the appearance of analyticity restrictions on the functions upon which the non-degenerate principal series of representations of $SL(n,\boldsymbol{R})$ act. Their argument runs as follows: Let $K(n,\boldsymbol{C})$ be the subgroup of $SL(n,\boldsymbol{C})$ consisting of the superdiagonal matrices of determinant unity. The non-degenerate principal series of representations of $SL(n,\boldsymbol{C})$ is realized in a space of functions defined on the right coset space $SL(n,\boldsymbol{C})/K(n,\boldsymbol{C})$, or alternately in a space of functions defined on $SL(n,\boldsymbol{C})$ which are (left) invariant under the action of $K(n,\boldsymbol{C})$. Now the non-degenerate principal series of $SL(n,\boldsymbol{R})$ may be thought of as acting in spaces of functions on $SL(n,\boldsymbol{R})$ which are invariant under the (left) action of a subgroup of $SL(n,\boldsymbol{C})$ of the form $xK(n,\boldsymbol{C})x^{-1}$, $x \in SL(n,\boldsymbol{C})$. This statement is to be interpreted as honest invariance under $SL(n,\boldsymbol{R}) \cap xK(n,\boldsymbol{C})x^{-1}$ together with differential left invariance under the Lie algebra of $xK(n,\boldsymbol{C})x^{-1}$, regarded as a complex subalgebra of the complexification of the Lie algebra of $SL(n,\boldsymbol{R})$. If the functions are taken to be defined on

$$\mathfrak{M} = SL(n,\boldsymbol{R})/[SL(n,\boldsymbol{R}) \cap xK(n,\boldsymbol{C})x^{-1}],$$

then invariance under the action of the Lie algebra goes over into analyticity on certain complex submanifolds of $\mathfrak{M}$.

Now it is known that the non-degenerate principal series of $SL(n,\boldsymbol{C})$ consists exactly of the representations of $SL(n,\boldsymbol{C})$ induced by characters of $K(n,\boldsymbol{C})$ in the sense of Mackey [5]. It is therefore natural to ask for a generalization of the notion of induced representation which for the case at hand gives the non-degenerate principal series of $SL(n,\boldsymbol{R})$. Our generalization has as its setting a Lie group G with Lie algebra $\mathfrak{g}$, a complex subalgebra $\mathfrak{n}$ of the complexification $\mathfrak{g}_c$ of $\mathfrak{g}$, a closed subgroup Γ of G whose Lie algebra

---

* Received January 13, 1961.

[1] Research supported by the National Science Foundation under grant NSF-G12165.

[2] Numbers in brackets refer to the bibliography at the end of the paper.

is $\mathfrak{g} \cap \mathfrak{n}$, a unitary representation L of Γ on a finite dimensional Hilbert space $\mathfrak{V}$, and a representation ρ of $\mathfrak{n}$ on $\mathfrak{V}$. Certain restrictions are placed on $\mathfrak{n}$ and ρ (for exact statements, see Section 3). The corresponding induced representation $U^{L,\rho}$ is a subrepresentation of the representation U^{L} (see [1] for the definition). Here too analyticity restrictions appear on the functions upon which $U^{L,\rho}$ operates (Proposition 2). Finally, the representations of Gelfand and Graev are of the form we propose, except for certain degenerate cases.

Section 2 develops the necessary preliminary material on manifolds with some real and some complex parameters. Theorem 1 gives us a way of producing such manifolds. In Section 3, we introduce our induced representations. The problem of calculating intertwining numbers is the subject of Section 4. The basic result is Theorem 3 and is based on the intertwining number theorem in [1]. (Applications of Theorem 3 to the various series of representations of the real semi-simple groups is reserved to another paper.) In Section 5, additional restrictions on the complex subalgebras involved allows us to reduce the intertwining number problem to one of solving certain differential equations, while Theorem 4 gives us effective irreducibility and disjointness criteria for the representations arising from this restricted class of subalgebras. Finally, in Section 6, we consider two examples:

(a) Harish-Chandra has also considered the problem of generalizing the notion of induced representation in case G is a semisimple Lie group and Γ is a special sort of Cartan subgroup. His results may be found in [4]. Our irreducibility and inequivalence criteria are applied to his representations.

(b) In [3], Gelfand and Graev mention a series of representations of $SL(2k, \boldsymbol{R})$ which are not in the non-degenerate principal series. Once again our irreducibility and inequivalence criteria apply.

2. Partially complex manifolds.

We begin by laying down some conventions and recalling some facts.

Vector spaces. If $\mathfrak{W}$ is a complex vector space, then $\mathfrak{W}_r$ will denote the real vector space obtained from $\mathfrak{W}$ by restricting the field of scalars. If $\mathfrak{W}$ is a real vector space, then $\mathfrak{W}_c$ is the complexification of $\mathfrak{W}$, and $\mathfrak{W}$ will be regarded as a real subspace of $\mathfrak{W}_{cr}$. In $\mathfrak{W}_c$, $^{+}$ will denote the unique conjugate linear isomorphism which $= -I$ on $\mathfrak{W}$. if Ψ is a linear map of the real vector space $\mathfrak{V}$ into the real vector space $\mathfrak{W}$, then Ψ_c will denote the usual extension of Ψ to a complex linear map of $\mathfrak{V}_c$ into $\mathfrak{W}_c$. If $\mathfrak{W}$ is a complex vector space, then κ is the unique complex linear map of $\mathfrak{W}_{rc}$ onto $\mathfrak{W}$

which leaves every point of $\mathfrak{W}_r = \mathfrak{W}$ fixed. If $\mathfrak{V}$ and $\mathfrak{W}$ are complex vector spaces and if Ψ is a linear map from $\mathfrak{V}_r$ into $\mathfrak{W}_r$, then Ψ is a complex linear if and only if Ψ_c carries $\ker(\kappa)$ into $\ker(\kappa)$.

Differentiable Manifolds. All functions and vector fields will be assumed to have open domains unless otherwise stated. Let $\mathcal{M}$ be a manifold. If $p \in \mathcal{M}$, then $\mathcal{M}_p$ will denote the tangent space to $\mathcal{M}$ at p. If f is a differentiable function from $\mathcal{M}$ to a complex vector space, if $p \in \operatorname{dom}(f)$, and if $X_p \in \mathcal{M}_{pc}$, then $X_p f$ is defined in the obvious way. A *complex distribution* of dimension r on $\mathcal{M}$ is a function $\mathfrak{m}$ from $\mathcal{M}$ to $\bigcup_{p \in \mathcal{M}} \mathcal{M}_{pc}$ such that $\mathfrak{m}_p$ (the value of $\mathfrak{m}$ at p) is an r-dimensional complex subspace of $\mathcal{M}_{pc}$; the properties of being analytic, involutive, etc., are defined in the obvious way. If ϕ is a differentiable map of $\mathcal{M}$ into another differentiable manifold, then ϕ_* will denote the induced map of tangent spaces.

Complex manifolds. Let $\mathcal{M}$ be equipped with a complex structure. Then $\mathcal{M}_p{}^c$ will denote $\mathcal{M}_p$ equipped with the canonically induced complex linear structure. To each $p \in \mathcal{M}$ we assign $\mathfrak{c}$, the kernel of κ in $\mathcal{M}_{pc}$ $(= \mathcal{M}_p{}^c{}_{rc})$. $\mathfrak{c}$ is a complex C^ω involutive distribution called the *canonical distribution* of $\mathcal{M}$. If ϕ is a differentiable map of $\mathcal{M}$ into another complex manifold, then ϕ is called *holomorphic* if ϕ_* is complex linear. This is equivalent to demanding that ϕ_{*c} take $\mathfrak{c}_p$ into $\mathfrak{c}_{\phi(p)}$ for all $p \in \operatorname{dom}(\phi)$. If f is a function from $\mathcal{M}$ to a complex vector space, then f is holomorphic in the above sense if and only if $\mathfrak{c}_p f = 0$ for all $p \in \operatorname{dom}(f)$ (Cauchy-Riemann equations). If X is a vector field with values in $\mathcal{M}_{pc}$, $p \in \mathcal{M}$, then X will be called *holomorphic* if Xf is holomorphic for all holomorphic functions with values in $\boldsymbol{C}$.

Mixed spaces. The canonical projection of $\boldsymbol{C}^m \times \boldsymbol{R}^n$ onto $\boldsymbol{C}^m$ (resp. $\boldsymbol{R}^n$) will be denoted θ (resp. ρ). If $x \in \boldsymbol{R}^n$, then θ_x will denote the map $z \to (z, x)$ of $\boldsymbol{C}^m$ into $\boldsymbol{C}^m \times \boldsymbol{R}^n$.

Our basic notion, that of a partially complex structure on a differentiable manifold, is to the mixed space $\boldsymbol{C}^m \times \boldsymbol{R}^n$ as the notion of complex structure is to the space $\boldsymbol{C}^m$.

Definition. Let $\mathcal{M}$ be a real C^ω manifold of dimension n. A partially complex structure of dimension r $(2r \leqq n)$ on $\mathcal{M}$ is a maximal collection $\mathcal{B}$ of maps satisfying:

(1) each $\phi \in \mathcal{B}$ is a C^ω diffeomorphism of an open set in $\mathcal{M}$ with an open set in $\boldsymbol{C}^r \times \boldsymbol{R}^{n-2r}$;

(2) the domains of the $\phi \in \mathcal{B}$ cover $\mathcal{M}$;

(3) if $\phi, \psi \in \mathcal{B}$ and $x \in \mathbf{R}^{n-2r}$, then $\rho \circ \phi \circ \psi^{-1}$ depends locally only on $\mathbf{R}^{n-2r}$ and $\theta \circ \phi \circ \psi^{-1} \circ \theta_x$ is holomorphic.

Remark. As usual, if $\mathcal{B}_0$ is any collection satisfying (1-3), then $\mathcal{B}_0$ is contained in a unique maximal collection $\mathcal{B}$ satisfying (1-3). Hence to define such a structure, we may ignore the maximality condition.

An open set O in $\mathcal{M}$ is called *cubical* if there is a coordinate function $\phi \in \mathcal{B}$ with domain O whose image is a set of the form $[(z_1, \cdots, z_r, x_1, \cdots, x_{n-2r}) : |z_i| < a, |x_i| < a]$ for some fixed $a > 0$.

We introduce a complex distribution $\mathfrak{m}$ as follows: if $\phi \in \mathcal{B}$ and $p \in \operatorname{dom} \phi$, then $\mathfrak{m}_p = \ker[(\rho \circ \phi)_{*c}] \cap (\theta \circ \phi)_{*c}{}^{-1}(\mathfrak{c}_{\theta(\phi(p))})$. It follows from condition (3) above that $\mathfrak{m}_p$ is independent of the choice of ϕ. From the way $\mathfrak{m}$ looks under ϕ_{*c} for a fixed $\phi \in \mathcal{B}$, it is clear that $\mathfrak{m}$ is involutive, that $\mathfrak{m} \cap \mathfrak{m}^+ = \{0\}$, and that $\mathfrak{m} + \mathfrak{m}^+$ is involutive, being in fact the complexification of the tangent distribution to slices of the form $[p \in \mathit{dom}\, \phi : \rho(\phi(p)) = \text{constant}]$. Each maximal integral manifold of $\mathfrak{m} + \mathfrak{m}^+$ is a complex manifold in the obvious fashion and will be called a *canonical complex submanifold* of $(\mathcal{M}, \mathcal{B})$.

THEOREM 1. *Let $\mathcal{M}$ be a real C^ω manifold of dimension n. Let $\mathfrak{m}$ be an involutive complex distribution $r (2r \leqq n)$ on $\mathcal{M}$ such that $\mathfrak{m} \cap \mathfrak{m}^+ = \{0\}$ and $\mathfrak{m} + \mathfrak{m}^+$ is involutive. Then $\mathcal{M}$ bears a unique partially complex structure $\mathcal{B}$ of dimension r such that $\mathfrak{m}$ is the canonical distrbution of $(\mathcal{M}, \mathcal{B})$.*

Proof. Let $p \in \mathcal{M}$. By the complex Frobenius Theorem there exists complex valued C^ω functions $f_1, \cdots, f_n$ defined in an open neighborhood N of p such that for all $q \in N$ the annihilators in $\mathcal{M}_{qc}$ of $\{f_1, \cdots, f_n\}$, $\{f_{r+1}, \cdots, f_n\}$, and $\{f_{2r+1}, \cdots, f_n\}$ are $\{0\}$, $\mathfrak{m}_q$, and $\mathfrak{m}_q + \mathfrak{m}_q{}^+$ respectively. Without loss of generality we may assume that N is a cubical neighborhood of breadth a about p with real coordinate functions $g_1, \cdots, g_n$ such that slices of the form $g_i(p) = \xi_i$, $|\xi_i| < a$, $i = 2r + 1, \cdots, n$ are integral manifolds of $\mathfrak{m} + \mathfrak{m}^+$. Set $\phi = (f_{r+1} \times \cdots \times f_{2r}) \times (g_{2r+1} \times \cdots \times g_n)$, a C^ω map of N into $\mathbf{C}^r \times \mathbf{R}^{n-2r}$. ϕ is regular. In fact, if $\phi_*(X_q) = 0$, $X_q \in \mathcal{M}_q$, $q \in N$, then $X_q \in \mathfrak{m} + \mathfrak{m}^+$ so that $X_q f_i = 0$ for $i = r + 1, \cdots, n$. Hence $X_q \in \mathfrak{m}_q \cap \mathcal{M}_q = \{0\}$. Shrinking N if necessary, we may assume that ϕ is a diffeomorphism of N with an open subset of $\mathbf{C}^r \times \mathbf{R}^{n-2r}$.

Let $\mathcal{B}_0$ be the collection of all ϕ's obtained in this fashion for arbitrary $p \in \mathcal{M}$. Properties 1 and 2 in the definition are true by construction. As for property 3, let $\phi, \psi \in \mathcal{B}_0$. Let $y \in \operatorname{dom}(\rho \circ \phi \circ \psi^{-1})$ and let N_0 be a neighborhood of $\psi^{-1}(y)$ such that $\psi(N_0)$ is a cube $\subseteq \operatorname{dom}(\rho\circ\phi\circ\psi^{-1})$. Then slices of N_0 of the form $[p\in N_0 : \rho(\psi(p)) = \text{constant}]$ are integral manifolds of $\mathfrak{m}+\mathfrak{m}^+$ contained in $\operatorname{dom}\phi$. Therefore $\rho\circ\phi$ is constant on these slices, and this implies that $\rho\circ\phi\circ\psi^{-1}$ restricted to $\psi(N_0)$ depends only on $\boldsymbol{R}^{n-2r}$. Now let $x\in\boldsymbol{R}^{n-2r}$, set $h=\theta\circ\phi\circ\psi^{-1}\circ\theta_x$, and let $z\in\operatorname{dom}h$. Observe that $(\psi^{-1}\circ\theta_x)_*$ maps $\mathfrak{c}_z$ univalently onto $\mathfrak{m}_{\psi^{-1}(z,x)}$ and that $(\theta\circ\phi)_*$ maps this space in turn univalently onto $\mathfrak{c}_{h(z)}$. Since h_* maps $\mathfrak{c}_z$ into $\mathfrak{c}_{h(z)}$, we conclude that h is holomorphic.

If $\mathcal{B}$ is the partially complex structure on $\mathcal{M}$ determined by $\mathcal{B}_0$, it is clear that $\mathfrak{m}$ is the canonical distribution of $(\mathcal{M},\mathcal{B})$. As for uniqueness, let $\mathcal{B}'$ be any partially complex structure satisfying the conclusion of the theorem and let $\phi\in\mathcal{B}_0$. The arguments of the last paragraph show that $\mathcal{B}'\cup\{\phi\}$ also satisfy the theorem. By maximality we conclude that $\mathcal{B}=\mathcal{B}'$.

3. The induced representations. For any unexplained notation concerning induced representations the reader is referred to [1]. Let G be a Lie group with left invariant Lie algebra $\mathfrak{g}$ and modular functions Δ. If $X\in\mathfrak{g}$ and $x(.)$ is the one-parameter subgroup of G lying beneath X, we have $(Xf)(y)=D_tf(yx(t))|_{t=0}$ for all differentiable functions f. We define a mapping $'$ of the family of differentiable functions onto itself by $f'(x)=f(x^{-1})$. Clearly $'$ is involutive. If X is a differential operator on G with C^∞ coefficients, we define $X^\square$ by $X^\square f=(Xf')'$ for all C^∞ functions f. $\square$ is clearly an involutive automorphism of the algebra of all C^∞ everywhere defined differential operators on G. If $X\in\mathfrak{g}$ and $x(.)$ lies beneath X, we have $(X^\square f)(y)=-D_tf(x(t)y)|_{t=0}$.

Let Γ be a closed subgroup of G with Lie algebra $\mathfrak{h}$ and modular function δ. Let $\mathfrak{n}$ be a complex subalgebra of $\mathfrak{g}_c$ such that $\mathfrak{n}\cap\mathfrak{n}^+=\mathfrak{h}_c$, $(\operatorname{ad}\Gamma)\mathfrak{n}=\mathfrak{n}$, and $\mathfrak{n}+\mathfrak{n}^+$ is a Lie algebra. Let $\mathcal{M}=G|\Gamma$ and let π be the canonical projection of G onto $\mathcal{M}$.

PROPOSITION 1. *$\pi_*(\mathfrak{n}^\square_x)$ depends only on $\pi(x)$. Moreover, if we set $\mathfrak{m}_p=\pi_*(\mathfrak{n}^\square_x)$ where $\pi(x)=p$, then $\mathfrak{m}$ is the canonical distribution of a unique partially complex structure $\mathcal{B}$ on $\mathcal{M}$.*

Proof. Let $X\in\mathfrak{g}$ and $x(.)$ be the one-parameter subgroup of G lying beneath X. Let f be a differentiable function on $\mathcal{M}$. Then

$$\begin{aligned}\pi_*(X^\square_{\xi g})f &= X^\square_{\xi g}(f\circ\pi) = -D_tf(\pi(x(t)\xi g))|_{t=0}\\ &= -D_tf(\pi(\xi^{-1}x(t)\xi g))|_{t=0} = \pi_*(\operatorname{ad}\xi^{-1}X)^\square_g)f\end{aligned}$$

for $\xi \in \Gamma$, $g \in G$. Since $(\mathrm{ad}\,\Gamma)\mathfrak{n} = \mathfrak{n}$, we conclude the truth of our first assertion.

Since the kernel of $\pi_* | \mathfrak{n}^{\square}_x$ is just $\mathfrak{h}_x = \mathfrak{n}_x \cap \mathfrak{n}_x^+$, we see that $\mathfrak{m} \cap \mathfrak{m}^+ = \{0\}$. If α is a local cross-section of G over $\mathcal{M}$, then $\alpha_*(\mathfrak{m}_p) = \mathfrak{n}^{\square}_{\alpha(p)}$ and

$$\alpha_*(\mathfrak{m}_p + \mathfrak{m}_p{}^+) = \mathfrak{n}^{\square}_{\alpha(p)} + \mathfrak{n}^{\square}_{\alpha(p)}{}^+ = (\mathfrak{n} + \mathfrak{n}^+)^{\square}_{\alpha(p)}$$

for all $p \in \mathrm{dom}(\alpha)$. It follows from [2], Ch. III, § 5, Proposition 2, that $\mathfrak{m}$ and $\mathfrak{m} + \mathfrak{m}^+$ are involuntary. Our second assertion now follows from Theorem 1.

Our induced representations are obtained as follows: Let L be a unitary representation of Γ on the finite dimensional Hilbert space $\mathfrak{B}$ and set $M(\xi) = \delta(\xi)^{\frac{1}{2}}\Delta(\xi)^{-\frac{1}{2}}L(\xi)$. Let ρ be a representation of $\mathfrak{n}$ on $\mathfrak{B}$ such that $\rho | \mathfrak{h} = dM$ and $\rho(\mathrm{ad}\,\xi X) = M(\xi)\rho(X)M(\xi)^{-1}$ for $\xi \in \Gamma$ and $X \in \mathfrak{n}$. As in [1], form the space $\mathfrak{F}$ of functions from G to $\mathfrak{B}$ determined by Γ and L. This paper, we shall denote this space by $\mathfrak{F}^L$ to show its dependence on L. Let $\mathfrak{F}^{L,\rho}$ be the linear space of all $f \in \mathfrak{F}^L$ such that

(1) the restriction of f to any integral manifold of $\mathfrak{n}^{\square} + \mathfrak{n}^{\square+}$ is of class C^{ω}, and

(2) $[X^{\square} + \rho(X)]f = 0$ for all $X \in \mathfrak{n}$.

It is possible that $\mathfrak{F}^{L,\rho} = \{0\}$. In any case, condition (2) is automatically satisfied for $X \in \mathfrak{h}_0$ by any $f \in \mathfrak{F}^L$. It is easy to see that U^L sends $\mathfrak{F}^{L,\rho}$ into itself. The restriction of U^L to $\mathfrak{F}^{L,\rho}$ (or rather to $\mathfrak{H}^{L,\rho}$, the corresponding pre-Hilbert space) is called the *representation of G induced by L and ρ*. It is denoted $U^{L,\rho}$.

In order to show that $\mathfrak{H}^{L,\rho}$ is complete, we shall characterize the $f \in \mathfrak{F}^{L,\rho}$ in terms of our partially complex structure $\mathcal{B}$ on $\mathcal{M}$. By a *charting function* for L and ρ will be meant a C^{ω} function H with values in $GL(\mathfrak{B})$ such that:

(1) $\mathrm{dom}(H) = \pi^{-1}(O)$, where O is some relatively compact cubical neighborhood in $(\mathcal{M}, \mathcal{B})$ over which is defined a C^{ω} cross-section in G;

(2) $H(\xi x) = M(\xi)H(x)$ for $\xi \in \Gamma$, $x \in \pi^{-1}(O)$; and

(3) $[X^{\square} + \rho(X)]H = 0$ on $\pi^{-1}(O)$ for all $X \in \mathfrak{n}$.

LEMMA 1. *Let $p_0 \in \mathcal{M}$. There exists a charting function H such that $p_0 \in \pi(\mathrm{dom}(H))$.*

Proof. Let O_1 be a relatively compact cubical neighborhood of p_0 over which a C^{ω} cross-section α into G is defined. Then the map $\omega\colon \Gamma \times O_1$ into

G given by $\omega(\xi, p) = \xi\alpha(p)$ is a C^ω diffeomorphism $\Gamma \times O_1$ with $\pi^{-1}(O_1)$. Now equations (3) are C^ω, non-singular, and satisfy the (complex) condition of Frobenius for local integrability. Hence there is a neighborhood N of $\alpha(p_0)$ for which a C^ω function H_1 from N to $GL(\mathfrak{B})$ is defined satisfying (3). Moreover, we may assume that $N = \omega(U \times O)$, where U is a cubical neighborhood of e in Γ and O is a cubical neighborhood of p_0. We define H on $\pi^{-1}(O)$ by $H(\xi\alpha(p)) = M(\xi)H_1(\alpha(p))$ for all $\xi \in \Gamma$ and $p \in O$. Note that H coincides with H_1 on N since (3) implies (2) whenever x and $\xi x \in N$, $\xi \in \Gamma$ (connectivity implies $\xi \in \Gamma_0$). H satisfies (2) by construction and satisfies (3) in N. Now if $X \in \mathfrak{g}$ and $x(.)$ is the 1-parameter subgroup of G lying beneath X, we have

$$\begin{aligned}(X^{\square}H)(\xi g) &= -D_t[H(x(t)\xi g)]\big|_{t=0} \\ &= -D_t[H(\xi\cdot\xi^{-1}x(t)\xi g]\big|_{t=0} = M(\xi)[(\operatorname{ad}\xi^{-1}X)^{\square}H](g),\end{aligned}$$

for $\xi \in \Gamma$, $g \in \pi^{-1}(O)$. Moreover

$$\rho(X)H(\xi g) = M(\xi)M(\xi)^{-1}\rho(X)M(\xi)H(g) = M(\xi)\rho(\operatorname{ad}\xi^{-1}X)H(g)$$

for $X \in \mathfrak{n}$. Since $(\operatorname{ad}\Gamma)(\mathfrak{n}) = \mathfrak{n}$, we conclude that H satisfies (3) in $\Gamma N = \pi^{-1}(O)$.

Fix a charting function H with domain $\pi^{-1}(O)$. Let f be a measurable function from $\pi^{-1}(O)$ to $\mathfrak{B}$. f satisfies condition (1) in the definition of $\mathfrak{F}^{L,\rho}$ if and only if $H^{-1}f$ does. Moreover

$$\begin{aligned}[X^{\square} + \rho(X)]f &= [X^{\square} + \rho(X)](HH^{-1}f) \\ &= ([X^{\square} + \rho(X)]H)(H^{-1}f) + H[X^{\square}(H^{-1}f)] = H[X^{\square}(H^{-1}f)]\end{aligned}$$

for all $X \in \mathfrak{n}$. Hence f satisfies (2) in the definition of $\mathfrak{F}^{L,\rho}$ if and only if $X^{\square}(H^{-1}f) = 0$ for all $X \in \mathfrak{n}$. Now if $f \in \mathfrak{F}^L$, then $H^{-1}f$ is a measurable function $\pi^{-1}(O)$ to $\mathfrak{B}$ which is constant on the right Γ cosets of G. Thus $H^{-1}f = {}^{H}f \circ \pi$, where ${}^{H}f$ is a unique measurable function from O to $\mathfrak{B}$. It is easily see that $H^{-1}f$ satisfies condition (1) in the definition of $\mathfrak{F}^{H,\rho}$ if and only if ${}^{H}f$ is of class C^ω on the integral manifolds of $\mathfrak{m} + \mathfrak{m}^{+}$. Moreover $\mathfrak{n}^{\square}(H^{-1}f) = 0$ if and only if $\mathfrak{m}\,{}^{H}f = 0$. We have proved

PROPOSITION 2. *Let $\mathfrak{D}$ be a collection of charting functions for L and ρ such that $G = \cup[\operatorname{dom}(H) : H \in \mathfrak{D}]$. Let $f \in \mathfrak{F}^L$. Then $f \in \mathfrak{F}^{L,\rho}$ if and only if ${}^{H}f$ is a complex analytic function on the canonical complex submanifolds of $(\mathcal{M}, \mathcal{B})$ for all $H \in \mathfrak{D}$.*

Let H be a charting function for L and ρ. Let ϕ be a coordinate map in $\mathcal{B}$ with domain $\pi(\operatorname{dom}(H))$ and image O. Let α be a cross-section of G

over $\pi(\operatorname{dom}(H))$ and let $\beta = \alpha \circ \phi^{-1}$. Let ω be the homeomorphism of $\Gamma \times O$ onto $\operatorname{dom}(H)$ given by $\omega(\xi, p) = \xi\beta(p)$. Let μ be the measure on $\Gamma \times O$ induced under ω by right Haar measure on G, and let γ be the density of μ with respect to the cartesian product of right Haar measure on Γ by Lebesgue measure on O. We know that $\gamma(\xi, p) = \delta(\xi)^{-1}\Delta(\xi)\gamma(e, p)$ for $\xi \in \Gamma$ and $p \in O$[1]. Finally, for each compact $K \subseteq O$ let

$$R_k = \operatorname{Min}[\gamma(e,p) \| H(\beta(p))^{-1} \|^{-2} : p \in K].$$

Let $f \in \mathfrak{F}^L$ and let K be a compact set in O. Choose $h \in C^+{}_0(\operatorname{dom}(H))$ such that $0 \leqq \tau h \leqq 1$ and $\tau h = 1$ on K. Then

$$\begin{aligned}
\| f \|^2 &\geqq \int_{\mathfrak{M}} \tau h \, d\mu_f = \int_G \| f(x) \|^2 h(x)\, dx \\
&= \int_{\pi^{-1}(K)} \| H(x)\, {}^H f(\pi(x)) \|^2 h(x)\, dx \\
&\geqq \int_K \int_\Gamma \| H(\xi\beta(p))^{-1} \|^{-2} \| {}^H f(\phi^{-1}(p)) \|^2 h(\xi\beta(p)) \gamma(\xi, p)\, d\xi\, dp \\
&\geqq R_K \int_K \| {}^H f(\phi^{-1}(p)) \|^2 dp
\end{aligned}$$

because $\| H(\xi\beta(p))^{-1} \|^{-2} \gamma(\xi, p)$ is independent of ξ and $\tau h = 1$ on K.

If $\{f_n\} \subseteq \mathfrak{H}^{L,\rho}$ and $f_n \to f \in \mathfrak{H}^L$, we have, for each compact $K \subseteq O$, that ${}^H f_n \circ \phi^{-1}$ and ${}^H f \circ \phi^{-1}$ are in $L_2(K)$ and that ${}^H f_n \circ \phi^{-1} \to {}^H f \circ \phi^{-1}$ in $L_2(K)$. Moreover ${}^H f_n \circ \phi^{-1}$ is complex analytic in its complex parameters, whence ${}^H f$ is complex analytic on the canonical complex submanifolds of $(\mathcal{M}, \mathcal{B})$. Applying Lemma 1 and Proposition 2, we obtain

THEOREM 2. *$\mathfrak{H}^{L,\rho}$ is complete and $U^{L,\rho}$ is a unitary representation of G on $\mathfrak{H}^{L,\rho}$.*

4. An intertwining number theorem. Suppose now that with G we are given two collections $\{\Gamma_i, \delta_i, \mathfrak{n}_i, \mathfrak{B}_i, L_i, \rho_i\}$, $i = 1, 2$, satisfying the conditions of the previous section. We wish to calculate an upper bound on the dimension $I(U^{L_1,\rho_1}, U^{L_2,\rho_2})$ of the space $\mathcal{R}(U^{L_1,\rho_1}, U^{L_2,\rho_2})$ of operators intertwining U^{L_1,ρ_1} and U^{L_2,ρ_2}. We shall be aided in this by the fact that U^{L_i,ρ_i} is a subrepresentation of U^{L_i}. Define the (non-unitary) representation M_i corresponding to L_i as in Section 3. For $f \in C_0{}^\infty(G)$ and $v \in \mathfrak{B}_i$, set

$$\epsilon_i{}^0(f, v)(x) = \int_{\Gamma_i} f(\xi x) M_i(\xi)^{-1} v \, d\xi.$$

Let P_i be the projection of H^{L_i} ond H^{L_i,ρ_i} and define $\epsilon_i(f,v)=P_i\epsilon_i^0(f,v)$. If $A\in\mathcal{R}(U^{L_1},U^{L_2})$, $f\in C_0^\infty(G)$, and $v\in\mathfrak{B}_1$, set $r^0{}_A(f)v=(A\epsilon_1^0(f,v))(e)$. This definition makes sense: see [1], § 5. If $A\in\mathcal{R}(U^{L_1,\rho_1},U^{L_2,\rho_2})$, then $AP_1=P_2AP_1\in\mathcal{R}(U^{L_1},U^{L_2})$ so that we may set $r_A(f)v=r^0{}_{AP_1}(f)v$. If $x,y\in G$, we set $(\zeta_{x,y}f)(z)=f(x^{-1}zy)$ for $f\in C_0^\infty(G)$.

If S is an operator mapping $C_0^\infty(G)$ into itself, the operator ${}^tS$, if it exists, will be defined by the identity $\int(Sf)(x)g(x)dx=\int f(x)({}^tSg)(x)dx$ for all $f,g\in C_0^\infty(G)$. It is easy to check that if $X\in\mathfrak{g}_c$ and $x,y\in G$, then ${}^tX=-X$, ${}^t(X^\Box)=-X^\Box+(X\Delta)(e)$, and ${}^t\zeta_{x,y}=\Delta(x)\zeta_{x^{-1},y^{-1}}$. If Z is any vector-valued distribution (in the sense of Schwartz [6]) on G, we set $SZ=Z\circ{}^tS$. Finally, any locally integrable function F on G will be identified with the distribution $f\to\int f(x)F(x)dx$.

Our intertwining number theorem now goes as follows:

THEOREM 3. *Let X_0 be an element of the universal associative enveloping algebra of $\mathfrak{g}$ which, as a left invariant differential operator on G, is elliptic of order $>\frac{1}{2}\dim(G/\Gamma_2)$. For $f\in C_0^\infty(G)$, set $\|f\|_{X_0}=\|X_0f\|_\infty+\|f\|_\infty$. For each relatively compact open set O of G, give $C_0^\infty(O)$ the topology induced by $\|\,.\,\|_{X_0}$; give $C_0^\infty(G)$ the inductive limit topology. Let $\mathfrak{M}$ be the subspace of maps $Z\in\mathcal{L}(C_0^\infty(G);\ \mathcal{L}(\mathfrak{B}_1,\mathfrak{B}_2))$ which satisfy the distribution equations:*

(1) $\zeta_{\xi_1,\xi_2}Z=M_2(\xi_2)^{-1}ZM_1(\xi_1)^{-1*}$ *for* $\xi_i\in\Gamma_i$;

(2) $X^{\Box+}Z=Z\rho_1(X)^*$, $X\in\mathfrak{n}_1$;

(3) $XZ=-\rho_2(X)Z$, $X\in\mathfrak{n}_2$.

Then $I(U^{L_1,\rho_1},U^{L_2,\rho_2})\leqq\dim\mathfrak{M}$.

Proof. From [1], Theorem 3, we deduce that $A\to r_A$ is a faithful linear map of $\mathcal{R}(U^{L_1,\rho_1},U^{L_2,\rho_2})$ into the subspace of maps $Z\in\mathcal{L}(C_0^\infty(G);\mathcal{L}(\mathfrak{B}_1;\mathfrak{B}_2))$ satisfying (1). To show that r_A satisfies (2), we note that

$$(\epsilon_1(f,v),g)=\int_G f(x)(v,g(x))dx$$

for $f\in C_0^\infty(G)$, $v\in\mathfrak{B}_1$, and $g\in\mathfrak{F}^{L_1,\rho_1}$. This follows immediately from the definition of ϵ_1 and the proof of Lemma 2(a) in [1]. Now $(v,g(\,.\,))$, regarded as a distribution on G, satisfies the equation $X^{\Box+}(v,g(\,.\,))=(\rho_1(X)^*v,g(\,.\,))$ for $X\in\mathfrak{n}_1$, in virtue of properties (1) and (2) of $\mathfrak{F}^{L_1,\rho_1}$. Therefore,

$$\begin{aligned}(\epsilon_1({}^tX^{\Box+}f,v),g)&=\int({}^tX^{\Box+}f)(x)(v,g(x))dx\\&=\int f(x)(\rho_1(X)^*v,g(x))dx=(\epsilon_1(f,\rho_1(X)^*v),g).\end{aligned}$$

From this we obtain

$$\begin{aligned}(X^{\square+}r_A)(f)v &= (A\epsilon_1({}^tX^{\square+}f,v))(e)\\ &= (A\epsilon_1(f,\rho_1(X)^*v))(e) - r_A(f)\rho_1(X)^*v\end{aligned}$$

for $X \in \mathfrak{n}_1$.

As for property (3), we recall from the proof of Theorem 3 in [1] that $r_A(\zeta_{e,y}f)v = (A\epsilon_1(f,v))(y)$ for all $y \in G$. Now the mapping $y \to \zeta_{e,y}f$ is a C^∞ map of G into $C_0{}^\infty(G)$. Since r_A is continuous and linear, we see that $(A\epsilon_1(f,v))(.)$ is a C^∞ function and that $r_A(Xf)v = [X(A\epsilon_1(f,v))](e) = -[X^\square(A\epsilon_1(f,v))](e)$ for all $X \in \mathfrak{g}_c$. If $X \in \mathfrak{n}_2$, we conclude that $r_A(Xf)v = \rho_2(X)r_A(f)v$.

5. Totally complex subalgebras. A complex subalgebra $\mathfrak{n}$ of $\mathfrak{g}_c$ will be called *totally complex* if $\mathfrak{n} + \mathfrak{n}^+ = \mathfrak{g}_c$.

PROPOSITION 3. *In Theorem 3, let either $\mathfrak{n}_1$ or $\mathfrak{n}_2$ be totally complex. Then $\mathfrak{M}$ consists entirely of C^ω functions.*

Proof. We shall give a proof for the case when $\mathfrak{n}_2$ is totally complex. The other case is entirely analogous. Let $\{X_1,\cdots,X_n\}$ be a basis for $\mathfrak{h}_2$, and extend it to a basis $\{X_1,\cdots,X_n,X_{n+1},\cdots,X_r\}$ of $\mathfrak{n}_2$. Then $\{X_1,\cdots,X_r,X_{n+1}{}^+,\cdots,X_r{}^+\}$ is a basis of $\mathfrak{g}_c$, by our assumption. If we write $X_j = Y_j + iZ_j$, where $Y_j, Z_j \in \mathfrak{g}$ for $j = \mathrm{n}+1,\cdots,r$, it follows that $\{X_1,\cdots,X_n,Y_{n+1},\cdots,Y_r,Z_{n+1},\cdots,Z_r\}$ is a basis of $\mathfrak{g}$. Now the differential operator $S = \sum_j{}^r{}_1 X_j{}^+(X_j + \rho_2(X_j)) = -\sum_j{}^n{}_1 X_j{}^2 - \sum_j{}^r{}_{n+1} Y_j{}^2 - \sum_j{}^r{}_{n+1} Z_j{}^2 +$ terms of lower order. This shows that S is elliptic (cf. [7]) and C^ω. If $Z \in \mathfrak{M}$, then $SZ = 0$ according to property (3) of $\mathfrak{M}$. Therefore, Z is a C^ω function (see p. 146 of [6] and the references given there).

Let $\mathfrak{n}$ be a totally complex subalgebra of $\mathfrak{g}_c$. We shall say that x is $\mathfrak{n}$-*regular* if $\mathfrak{n} + \operatorname{ad} x^{-1}\mathfrak{n}^+ = \mathfrak{g}_c$ and shall denote the set of $\mathfrak{n}$-regular elements by $R_{\mathfrak{n}}$.

LEMMA 2. *In Theorem 3 assume the following: G is connected; $\Gamma_1 = \Gamma_2 = \Gamma$, say; and $\mathfrak{n}_1 = \mathfrak{n}_2 = \mathfrak{n}$, say, a totally complex subalgebra of $\mathfrak{g}_c$. Let $Z \in \mathfrak{M}$ and suppose $Z(x_0) = 0$ for some $x_0 \in R_{\mathfrak{n}}$. Then $Z = 0$.*

Proof. We choose vector fields $X_1,\cdots,X_n \in \mathfrak{n}$ such that, for suitably chosen r, $\{X_1,\cdots,X_r,\operatorname{ad} x_0{}^{-1}X_{r+1}{}^+,\cdots,\operatorname{ad} x_0{}^{-1}X_n{}^+\}$ is a basis for $\mathfrak{g}_c$. It is then easy to see that there is a C^ω cubical neighborhood N about x_0 such that $\{X_1,\cdots,X_r,\operatorname{ad} x^{-1}X_{r+1}{}^+,\cdots,\operatorname{ad} x^{-1}X_n{}^+\}$ is a basis for $\mathfrak{g}_c$ for all $x \in N$. Let

$x_1, \cdots, x_n$ be the coordinate functions for N. There exist C^ω functions a_{ij} for $i, j = 1, \cdots, n$ such that, for all $x \in N$,

$$\left(\frac{\partial}{\partial x_i}\right)_x = \sum_j {}^{r}{}_{1}\, a_{ij}(x)\,(X_j)_x + \sum_j {}^{n}{}_{r+1}\, a_{ij}(x)\,(\operatorname{ad} x^{-1}X_j^+)_x.$$

Now for any $X \in \mathfrak{g}_c$, $(\operatorname{ad} x^{-1}X)_x = -X^{\square}{}_x$. Therefore

$$\frac{\partial Z}{\partial x_i} = -\sum_j {}^{r}{}_{1}\, a_{ij}(\,.\,)\rho_2(X_j)Z - \sum_j {}^{n}{}_{r+1}\, a_{ij}(\,.\,)Z\rho_1(X_j)^*$$

by virtue of Theorem 3. But $Z(x_0) = 0$. From the uniqueness theorem for ordinary linear differential equations we conclude that Z vanishes on N. Since Z is a C^ω function, Z vanishes identically on G.

We are now in a position to prove

THEOREM 4. *Suppose that G is connected and suppose the induced representations U^{L_1,ρ_1} and U^{L_2,ρ_2} satisfy the following conditions: L_1 and L_2 are defined on Γ; ρ_1 and ρ_2 are defined on $\mathfrak{n}$, a totally complex subalgebra of $\mathfrak{g}_c$. For each $x \in G$, define a representation ρ_{1x} of $\operatorname{ad} x^{-1}\mathfrak{n}^+$ by setting $\rho_{1x}(X) = \rho_1(\operatorname{ad} xX^+)^*$ for $X \in \operatorname{ad} x^{-1}\mathfrak{n}^+$, also a representation M_{1x} of $x^{-1}\Gamma x$ by setting $M_{1x}(\xi) = M_1(x\xi x^{-1})^{*-1}$ for $\xi \in x^{-1}\Gamma x$. Define $I(x)$ to be the dimension of $\mathfrak{R}_x$, where*

$$\mathfrak{R}_x = \mathfrak{R}\,(\rho_{1x}|\mathfrak{n} \cap \operatorname{ad} x^{-1}\mathfrak{n}^+, \rho_2|\mathfrak{n} \cap \operatorname{ad} x^{-1}\mathfrak{n}) \cap \mathfrak{R}\,(M_{1x}|\Gamma \cap x^{-1}\Gamma x, M_2|\Gamma \cap x^{-1}\Gamma x).$$

Then (1) *$I(x)$ depends only on the $\Gamma : \Gamma$ double coset to which x belongs and* (2) *$I(U^{L_1,\rho_1}, U^{L_2,\rho_2}) \leqq \mathrm{GLB}[I(x) : x \in R_{\mathfrak{n}}] < \infty$.*

Proof. First note that $e \in R_{\mathfrak{n}}$ so that $\mathrm{GLB}[I(x) : x \in R_{\mathfrak{n}}] < \infty$. Fix a point $x_0 \in R_{\mathfrak{n}}$. For each $Z \in M$, set $\Omega(T) = Z(x_0)$. The map $\Omega \in \mathscr{L}(\mathfrak{M}; \mathscr{L}(\mathfrak{B}_1; \mathfrak{B}_2))$.

(a) $\Omega \in \mathscr{L}(\mathfrak{M}; \mathfrak{R}_{x_0})$. In fact, let $Z \in \mathfrak{M}$. If $\xi \in \Gamma \cap x_0^{-1}\Gamma x_0$, then $x_0\xi x_0^{-1} \in \Gamma$ and $(x_0\xi x_0^{-1})x_0\xi^{-1} = x_0$. Property (1) of $\mathfrak{M}$ implies that $Z(x_0) = M_2(\xi)Z(x_0)M_1(x_0\xi x_0^{-1})^*$ so that $Z(x_0)M_{1x_0}(\xi) = M_2(\xi)Z(x_0)$. Again, if $X \in \mathfrak{n} \cap \operatorname{ad} x_0^{-1}\mathfrak{n}^+$, then $\operatorname{ad} x_0X^+ \in \mathfrak{n}$. Properties (2) and (3) of $\mathfrak{M}$ imply that

$$\begin{aligned} Z(x_0)\rho_{1x_0}(X) &= Z(x_0)\rho_1(\operatorname{ad} x_0X^+)^* \\ &= ([\operatorname{ad} x_0X]^{\square}Z)(x_0) = -(XZ)(x_0) = \rho_2(X)Z(x_0). \end{aligned}$$

Therefore $\Omega(Z) \in \mathfrak{R}_{x_0}$.

(b) Ω is one-to-one. In fact, suppose $\Omega(Z) = 0$. Then $Z(x_0) = 0$ so that $Z = 0$ by Lemma 3.

We have shown that Ω is an isomorphism of $\mathfrak{M}$ into $\mathfrak{R}_{x_0}$. This proves statement (2). The proof of statement (1) is standard and will be omitted.

COROLLARY 1. *In case* $\mathfrak{n}$ *is totally complex, a necessary condition for* $\mathfrak{H}^{L,\rho} \neq \{0\}$ *is that* $\delta = \Delta | \Gamma$.

Proof. In Theorem 4, let $\mathfrak{B}_1 = \mathfrak{B}_2 = \mathfrak{B}$, $L_1 = L_2 = L$, and $\rho_1 = \rho_2 = \rho$. If $\mathfrak{H}^{L,\rho} \neq \{0\}$, then $\mathfrak{M} \neq \{0\}$ so that $\mathfrak{R}_e \neq \{0\}$. Let $0 \neq S \in \mathfrak{R}_e$. Then, for all $\xi \in \Gamma$, $\delta(\xi)^{-\frac{1}{2}}\Delta(\xi)^{\frac{1}{2}}SL(\xi) = \delta(\xi)^{\frac{1}{2}}\Delta(\xi)^{-\frac{1}{2}}L(\xi)S$. It follows that

$$\delta(\xi)\Delta(\xi)^{-1} \| Sv \| = \| SL(\xi)v \| \leqq \| S \| \, \| v \|$$

for all $v \in \mathfrak{B}$. But this implies that $\delta(\xi)\Delta(\xi)^{-1} \| S \| \leqq \| S \|$ for all $\xi \in \Gamma$, and our conclusion follows.

COROLLARY 2. *Suppose* $\mathfrak{n}$ *is totally complex. If* L *is irreducible and if* $\mathfrak{H}^{L,\rho} \neq \{0\}$, *then* $U^{L,\rho}$ *is irreducible. If* L' *and* ρ' *are two more such representations defined on* Γ *and* $\mathfrak{n}$, *then* $U^{L',\rho'}$ *and* $U^{L,\rho}$ *are inequivalent if* L' *and* L *are inequivalent.*

Proof. Apply Theorem 4 to (L,ρ) *and* (L',ρ'). We get $I(U^{L,\rho}, U^{L',\rho'}) \leqq I(e)$, which equals 1 or 0 according as L and L' are equivalent or inequivalent. Our corollary follows immediately.

7. Some examples.

(a) Some representations of Harish-Chandra.

Let G be a real semi-simple Lie group and let Γ be a Cartan subgroup. In this case, $\Delta = 1$ and $\delta = 1$. We suppose that the image of Γ in the adjoint group of G is compact. Let $\mathfrak{g}$ (resp. $\mathfrak{h}$) be the Lie algebra of G (resp. Γ). $\mathfrak{h}_c$ is a Cartan subalgebra of $\mathfrak{g}_c$, and our assumption implies that every root of $\mathfrak{g}_c$ with respect to $\mathfrak{h}_c$ is purely imaginary on $\mathfrak{h}$. Let the roots be totally ordered in the usual way, and set $\mathfrak{n}$ equal to $\mathfrak{h}_c$ plus the space spanned by the root vectors belonging to the positive roots. Let X be a root vector belonging to the positive root α. Let $H \in \mathfrak{h}$. Then $[H, X^+] = -[H^+, X]^+ = [H, X]^+ = (\alpha(H)X)^+ = -\alpha(H)X^+$ since $\alpha(H)$ is pure imaginary. We see that $\mathfrak{n}^+$ is $\mathfrak{h}_c$ plus the space spanned by the root vectors belonging to the negative roots. We have that $\mathfrak{n}$ is a complex subalgebra of $\mathfrak{g}_c$, that $\mathfrak{n} + \mathfrak{n}^+ = \mathfrak{g}_c$, and that $\mathfrak{n} \cap \mathfrak{n}^+ = \mathfrak{h}_c$. Since Γ is connected, $(\operatorname{ad} \Gamma)\mathfrak{n} = \mathfrak{n}$.

Let χ be a character of the abeilan group Γ. $d\chi$ extends uniquely to a complex linear representation ρ of $\mathfrak{n}$ on $\boldsymbol{C}$: merely note that $\rho(X)$ must vanish whenever X is a root vector belonging to a positive root. *Let* χ *be the* *collection of all characters* χ *of* Γ *such that* $\mathfrak{H}^{\chi,\rho} \neq \{0\}$. *Then the representations* $U^{\chi,\rho}$ *for* $\chi \in \mathrm{X}$ *are all irreducible and mutually inequivalent.* The actual structure of X has been studied by Harish-Chandra in [4].

(b) Certain representations of $GL(2k, \boldsymbol{R})$.

Let $\mathfrak{W}$ be a real finite dimensional vector space and let $\mathfrak{g}$ be the Lie algebra of all $T \in \mathcal{L}(\mathfrak{W};\mathfrak{W})$ with vanishing trace. $\mathfrak{g}_c$ may then be identified with the Lie algebra of all $T \in \mathcal{L}(\mathfrak{W}_c;\mathfrak{W}_c)$ with vanishing trace. Suppose $\dim \mathfrak{W} = 2k$, k integral. It is then possible to choose vectors $v_1, \cdots, v_k \in \mathfrak{W}_c$ such that $\{v_1, \cdots, v_k, v_1^+, \cdots, v_k^+\}$ is a basis for $\mathfrak{W}_c$. Let $\mathfrak{n} = \{T \in \mathfrak{g}_c\colon v_j$ is an eigenvector of T for $j = 1, \cdots, k\}$, a Lie subalgebra $\mathfrak{g}_c$. Then $\mathfrak{h}_1 = \mathfrak{n} \cap \mathfrak{n}^+$ equals $\{T \in \mathfrak{g}_c\colon v_j$ and v_j^+ is an eigenvector of T for $j = 1, \cdots, k\}$, a Cartan subalgebra of $\mathfrak{g}_c$, and $\mathfrak{h} = \mathfrak{h}_1 \cap \mathfrak{g}$ is a Cartan subalgebra of $\mathfrak{g}$ such that $\mathfrak{h}_c = \mathfrak{h}_1$.

We define linear functionals $\lambda_1, \cdots, \lambda_k$ on $\mathfrak{n}$ by $Tv_j = \lambda_j(T)v_j$ for $T \in \mathfrak{n}$. It is easily seen that the derived algebra $\mathfrak{n}^{(2)}$ of $\mathfrak{n} = \{T \in \mathfrak{n}\colon \lambda_j(T) = 0$ for $j = 1, \cdots, k\}$. Our first object is to determine the space P of all homomorphisms of $\mathfrak{n}$ into $\boldsymbol{C}$ such that $\rho(T)$ is pure imaginary for $\rho \in \mathrm{P}$, $T \in \mathfrak{h}$.

LEMMA 3. $\mathrm{P} = \{a \sum_{j}{}^{k}{}_{1} \lambda_j\colon a \in \boldsymbol{R}\}$.

Proof. Clearly P is the set of all linear functionals ρ on $\mathfrak{n}$ such that $\rho(\mathfrak{n}^{(2)}) = 0$ and $\rho(T^+) = \overline{\rho(T)}$ for $T \in \mathfrak{h}_c$. We first show that $\sum_{j}{}^{k}{}_{1} \lambda_i \in \mathrm{P}$. Clearly $\sum_{j}{}^{k}{}_{1} \lambda_i(\mathfrak{n}^{(2)}) = 0$. Let $T \in \mathfrak{h}_c$. Then $T^+v_j^+ = -(Tv_j)^+ = -\overline{\lambda_i(T)}v_j^+$. Since T has vanishing trace, we conclude that $\sum_{j}{}^{k}{}_{1} \lambda_i(T^+) = \sum_{j}{}^{k}{}_{1} \overline{\lambda_j(T)}$.

Conversely, let $\rho \in \mathrm{P}_0$. Suppose $T \in \mathfrak{n}$ satisfies $\sum_{j}{}^{k}{}_{1} \lambda_j(T) = 0$. Define $S \in \mathcal{L}(\mathfrak{W}_c;\mathfrak{W}_c)$ by $Sv_j = \lambda_j(T)v_j$, $Sv_j^+ = 0$ for $j = 1, \cdots, k$. By assumption, $S \in \mathfrak{g}_c$ so that $S \in \mathfrak{h}_c$. It is also clear that $T - S$ and $S^+ \in \mathfrak{n}^{(2)}$. Therefore $\rho(T) = \rho(T - S) + \overline{\rho(S^+)} = 0$. We conclude that $\rho = a\sum_{j}{}^{k}{}_{1} \lambda_i$ for some $a \in \boldsymbol{C}$. If $T \in \mathfrak{h}_c$, then $\rho(T) = \overline{\rho(T^+)} = \bar{a}\sum_{j}{}^{k}{}_{1} \lambda_i(T)$. Since $\sum_{j}{}^{k}{}_{1} \lambda_j$ does not vanish on $\mathfrak{h}_c$, we see that $a \in \boldsymbol{R}$.

Let $G = SL(\mathfrak{W})$ and let Γ be the analytic subgroup of G lying beneath $\mathfrak{h}$. Let P_0 be the collection of all $\rho \in \mathrm{P}$ such that $\rho | \mathfrak{h} = d\chi$ for some (necessarily unique) character χ of Γ. $\mathfrak{n} = \mathfrak{h} + \mathfrak{n}^{(2)}$ implies that χ uniquely determines ρ. A necessary and sufficient condition that $\rho \in \mathrm{P}_0$ is that $\rho \in \mathrm{P}$ and $i\rho$ be integral on the kernel of the map $T \rightarrow \exp T$ of $\mathfrak{h}$ onto Γ, and this is easily seen to be equivalent to the requirement that $i\rho(T)$ be integral for all

$T \in \mathfrak{h}$ such that $\operatorname{Im} \lambda_j(T)$ is integral for $j = 1, \cdots, k$. But $T \to (\operatorname{Im} \lambda_1(T), \cdots, \operatorname{Im} \lambda_k(T))$ maps $\mathfrak{h}$ *onto* $\boldsymbol{R}^k$ because the trace restriction on $T \in \mathfrak{h}$ is just $\sum_j{}^k{}_1 \operatorname{Re} \lambda_j(T) = 0$. We conclude that $\rho \in \mathrm{P}_0$ if and only if $\rho = m \sum_j{}^k{}_1 \lambda_j$, where m is integral.

Since both G and Γ are unimodular and since Γ is connected, we obtain a series of representations $U^{\chi,\rho}$ of G, where $\rho \in \mathrm{P}_0$ and $d\chi = \rho | \mathfrak{h}$. If P_{00} is the set of $\rho \in \mathrm{P}_0$ for which $\mathfrak{H}^{\chi,\rho} \neq \{0\}$, we conclude from Corollary 2 of Theorem 4: *the representations* $U^{\chi,\rho}$ *for* $\rho \in \mathrm{P}_{00}$ *are all irreducible and mutually inequivalent.* These representations are mentioned by Gelfand and Graev in Subsection 4 of the Introduction of [3].

THE UNIVERSITY OF CALIFORNIA,
LOS ANGELES, CALIFORNIA.

REFERENCES.

[1] R. J. Blattner, "On induced representations," *American Journal of Mathematics*, vol. 83 (1961), pp. 79-98.

[2] C. Chevalley, *Theory of Lie Groups* I, Princeton University Press, 1946.

[3] I. M. Gelfand and M. I. Graev, "Unitary representations of the real unimodular group (principal nondegenerate series)," *Isvestiya Akademii Nauk SSSR. Seriya Matematičeskaya*, vol. 17 (1953), pp. 189-248.

[4] Harish-Chandra, "Representations of semisimple Lie groups. V," *American Journal of Mathematics*, vol. 78 (1956), pp. 1-41.

[5] G. W. Mackey, "Induced representations of locally compact groups I," *Annals of Mathematics*, vol. 55 (1952), pp. 101-159.

[6] L. Schwartz, *Théorie des distributions* I, Hermann, Paris, 1957.

[7] W. F. Stinespring, "Integrability of Fourier transforms for unimodular Lie groups," *Duke Mathematical Journal*, vol. 26 (1959), pp. 123-131.

ON SOME INTERPOLATION PROBLEMS FOR ANALYTIC FUNCTIONS.*

By H. S. Shapiro and A. L. Shields.[1]

In the first part of this paper we consider an interpolation problem for bounded analytic functions that was first solved by Lennart Carleson [3] (a detailed description is given below). We give a new proof of Carleson's result and we obtain analogous results for the spaces H_p. In the second part of the paper (Sections Four and Five) we study a related interpolation problem in certain Hilbert spaces of analytic functions, using the results obtained previously.

The interpolation problem for bounded functions has to do with the existence of sequences of points $\{z_n\}$ in the unit circle having the property that, given an arbitrary bounded sequence of complex numbers $\{w_n\}$, there is a bounded analytic function f for which

$$f(z_n) = w_n \qquad (n = 1, 2, \cdots).$$

If the sequence $\{z_n\}$ has this property we shall call it an *interpolating sequence.*

The problem of the existence of interpolating sequences was posed by R. C. Buck. The classical interpolation theory (see, for example, Nevanlinna [10] and Schur [15]) does not seem to be of help here. For example, Schur gives an explicit algorithm for finding the bounded function of minimal norm taking prescribed values $w_1, \cdots, w_n$ at the points $z_1, \cdots, z_n$. However, his method does not seem to lead to an effective estimate of this norm as n increases and as $\{w_n\}$ ranges over the unit sphere of l_∞.

Independently of one another L. Carleson [3], W. Hayman [6] and D. J. Newman [11] studied this problem. Carleson showed that a necessary and sufficient condition for $\{z_n\}$ to be an interpolating sequence is that there exist a positive number δ such that

$$\text{(C)} \qquad \prod_{n \neq k} |(z_k - z_n)/(1 - \bar{z}_n z_k)| \geq \delta \qquad (k = 1, 2, \cdots).$$

---

* Received January 24, 1961.

[1] The first author's contribution to this paper represents research done at the Institute of Methematical Sciences at New York University under the sponsorship of ONR contract N6 ori-201 (01).

The second author is a temporary member of the Institute of Mathematical Sciences; he also wishes to acknowledge contract AF 49 (638)-619.

Newman proved that condition (C) together with condition (H) given below are necessary and sufficient fo r$\{z_n\}$ to be an interpolating sequence:

$$\text{(H)} \qquad \sum |f(z_n)|(1-|z_n|) < \infty \qquad (\text{for all } f \in H_1).$$

Thus Carleson's result tells us that (C) implies (H), and in fact this is the heart of his proof.

Hayman showed that (C) is necessary and that a slight strengthening of it is sufficient. With his stronger condition he is able to give an explicit interpolation formula to find an f taking the given values $\{w_n\}$. He also shows that if one can interpolate arbitrary sequences of zeros and ones at the points $\{z_n\}$ then condition (C) is satisfied.

Both Newman and Hayman show that if z_n tend exponentially to the boundary, that is, if $\limsup(1-|z_{n-1}|)/(1-|z_n|) < 1$, then $\{z_n\}$ is an interpolating seqence. They point out that if the $\{z_n\}$ all lie on one radius, then this condition is also necessary.

Three years earlier, in connection with an interpolation problem for functions of bounded characteristic, A. G. Naftalevitch [9] showed that if $\{z_n\}$ satisfy the condition $\sum(1-|z_n|) < \infty$, then there exist points $\{z_n'\}$, with $|z_n'| = |z_n|$ $(n = 1, 2, \cdots)$, for which condition (C) is satisfied and for which

$$\text{(N)} \qquad \sum(1-|z_n|)\log^+|f(z_n)| < \infty$$

for all analytic f of bounded characteristic. He did not show that condition (N) is implied by condition (C).

Subsequently, V. Kabaila [7] pointed out that Naftalevitch's method shows that if $\sum(1-|z_n|) < \infty$, then there are points $\{z_n'\}$, with $|z_n'| = |z_n|$ $(n = 1, 2, \cdots)$, for which condition (H) is satisfied.

In Section Two of this paper we give a new proof of Carleson's result that $\{z_n\}$ is an interpolating sequence if and only if condition (C) is satisfied. We first show by a Banach space argument that, in the presence of condition (C), $\{z_n\}$ is an interpolating sequence if and only if condition (H) is satisfied. This part of the argument is similar to Carleson's proof, though differing in detail. We next show that (H) is equivalent to the following weighted interpolation problem in the space H_2:

For each sequence $\{c_n\} \in l_2$ there is an $f \in H_2$ for which

$$f(z_n)(1-|z_n|^2)^{\frac{1}{2}} = c_n \qquad (n = 1, 2, \cdots).$$

We complete the proof by showing that if condition (C) is satisfied then this weighted interpolation problem can be solved.

In Section Three we discuss weighted interpolation in the spaces H_p. We associate with each $f \in H_p$ the sequence of weighted values

$$T_pf = (f(z_1)(1-|z_1|)^{1/p}, f(z_2)(1-|z_2|)^{1/p}, \cdots),$$

and we consider the following two problems (as always, l_p denotes the space of sequences $\{c_n\}$ for which $\sum |c_n|^p < \infty$).

1. Is $l_p \subset T_pH_p$, that is, can one obtain arbitrary p-th power summable values by weighted interpolation using functions of class H_p?

2. Is $T_pH_p \subset l_p$, that is, do we have $\sum |f(z_n)|^p(1-|z_n|) < \infty$ for all $f \in H_p$?

One can show that if (1) is satisfied for some value of p $(1 \leqq p \leqq \infty)$, then condition (C) is satisfied. A Banach space argument shows that, in the presence of condition (C), (1) holds for a given value of p if and only if (2) holds for the conjugate index q $(1/p + 1/q = 1)$. The problem can then be reduced to the weighted interpolation problem in H_2 which was solved in Section Two. The final result is that for any given value of p $(1 \leqq p \leqq \infty)$ $T_pH_p = l_p$ if and only if the sequence $\{z_n\}$ satisfies condition (C).

In Section Four we consider for general Hilbert spaces of analytic functions a weighted interpolation problem analogous to the H_2 problem in Section Two. Certain equivalences are pointed out and an application is made to the H_2 interpolation problem in case the points z_n approach the boundary exponentially.

In Section Five we use the results on H_2 interpolation and the results of Section Four to study interpolation in two special Hilbert spaces: the space H_2' of functions that are derivatives of H_2 functions, and the space A_2 of functions with finite area norm: $\int\int |f(z)|^2 \, dxdy < \infty$. We show that if the points $\{z_n\}$ satisfy condition (C), then the weighted interpolation problem can be solved in each of these spaces.

Furthermore, a necessary condition for weighted interpolation in these spaces (and in H_2) is that the points $\{z_n\}$ be "weakly separated," that is, $|z_i - z_j| \geqq c(1-|z_i|)$ for some constant $c > 0$ and all i, j. If the $\{z_n\}$ all lie on one radius then this condition is equivalent to exponential approach to the boundary and is both necessary and sufficient. This is related to some results of Epstein, Greenstein, and Minker [4].

1. **Background material.** As usual H_p $(1 \leqq p < \infty)$ denotes the Banach space of functions f, analytic for $|z| < 1$, for which

$$\| f \|_p = \sup_r \{ \tfrac{1}{2\pi} \int_0^{2\pi} |f(re^{i\theta})|^p \, d\theta \}^{1/p} < \infty.$$

H_∞ will denote the bounded analytic functions with the supremum norm. For the properties of the spaces H_p see the book of Privaloff ([12], Chapters 1, 2). In particular we shall need the fact that H_p is isometric to a closed subspace of $L_p(0,2\pi)$ $(1 \leqq p \leqq \infty)$. If $f \in L_p$, $g \in L_q$ $(1/p + 1/q = 1)$, then we write

$$(1)\qquad (f,g) = \frac{1}{2\pi}\int_0^{2\pi} f(e^{i\theta})g(e^{i\theta})\,d(e^{i\theta}).$$

With this notation H_q is the annihilator of H_p: $H_q = H_p{}^{\perp}$ $(1 \leqq p < \infty)$. In the Hilbert space L_2 (1) is not an inner product.

Duality. Let E be a Banach space with conjugate space E^*. Let $F \subset E$ be a closed subspace and let $F^{\perp}$ be the set of all those elements of E^* that vanish on F. Then F^*, the conjugate space of F, can be identified with the quotient space $E^*/F^{\perp}$. The norm in the quotient space is given by

$$\| e^* + F^{\perp} \| = \inf \| e^* + \lambda \| \qquad (\lambda \in F^{\perp}).$$

On the other hand, the norm of a linear functional is the supremum of its values on the unit sphere, and so:

$$(2)\qquad \inf_{\lambda \in F^{\perp}} \| e^* + \lambda \| = \sup_{\substack{f \in F \\ \|f\|=1}} |(f, e^*)|.$$

It follows from the Hahn-Banach theorem that the infimum on the left is always attained.

Similarly, by considering E/F and its conjugate space $F^{\perp}$ we have:

$$(3)\qquad \inf_{f \in F} \| e + f \| = \sup_{\substack{\lambda \in F^{\perp} \\ \|\lambda\|=1}} |(e, \lambda)|.$$

The supremum on the right is always attained (since, in the weak star topology, the unit ball of $F^{\perp}$ is compact and e is continuous). See Havinson [5] and Rogosinski, Shapiro [13] for a discussion of these duality relations and their applications to extremal problems in H_p.

Quadratic forms. Let (a_{ij}) $(i, j = 1, 2, \cdots)$ be given. A result of Schur [14] states that if $\sum_i |a_{ij}| \leqq M$ for all j, and if $\sum_j |a_{ij}| \leqq N$ for all i, then

$$(4)\qquad \left|\sum_{i,j} a_{ij}x_i\bar{x}_j\right| \leqq (MN)^{\frac{1}{2}} \sum |x_i|^2.$$

2. Interpolation by bounded analytic functions. Let $\{z_n\}$ be a sequence of distinct points in the unit circle. Define a linear operator T from H_∞ to l_∞ (the bounded sequences) by

$$Tf = (f(z_1), f(z_2), \cdots).$$

Clearly $\| T \| = 1$. Note that if T is onto, then the interpolation can actually be done in a uniformly bounded manner, that is, there is a number M such that if $w = \{w_k\}$ is any element in the unit ball of l_∞, then there is an $f \in H_\infty$ with $Tf = w$ and $\| f \| \leqq M$.

Indeed, let N be the set of those $f \in H_\infty$ vanishing on $\{z_n\}$. Then N is a closed subspace and T induces a one-to-one continuous mapping from the quotient Banach space H_∞/N onto l_∞. By a theorem of Banach ([1], Chap. IV, Théorème 5) the inverse mapping is bounded, which is our assertion.

THEOREM 1. *A necesssary and sufficient condition for* $\{z_n\}$ *to be an interpolating sequence (that is,* $T(H_\infty) = l_\infty$*) is that*

$$(\mathrm{C}_1) \qquad \prod_{j \neq k} |(z_k - z_j)/(1 - \bar{z}_j z_k)| \geqq \delta > 0 \qquad (k = 1, 2, \cdots),$$

or equivalently,

(C_2) *there exist functions* $f_k \in H_\infty$ *such that*

(i) $f_k(z_l) = \delta_{lk}$,

(ii) $\| f \| \leqq 1/\delta \qquad (k = 1, 2, \cdots)$.

In this case each sequence $w = \{w_n\}$ *in the unit sphere of* l_∞ *can be interpolated by an* $f \in H_\infty$ *with*

$$(5) \qquad \| f \| \leqq (2/\delta^5)(1 - 2 \log \delta).$$

We shall use the following notations.

$$B_n(z) = \prod_1^n (z - z_j)/(1 - \bar{z}_j z),$$
$$B_{nk}(z) = B_n(z)(1 - \bar{z}_k z)/(z - z_k) \qquad (k \leqq n),$$
$$b_{nk} = B_{nk}(z_k).$$

The equivalence of conditions (C_1) and (C_2) is easy to see. Indeed, if (C_1) is given, then the Blaschke product formed from the points $\{z_n\}$ with the point z_k deleted, divided by its value at z_k, may be taken as the function f_k.

Conversely, if (C_2) is given then $\| f_k/B_{nk} \| = \| f_k \| \leqq 1/\delta$. Evaluation at z_k gives $1/|b_{nk}| \leqq 1/\delta$ which implies (C_1).

Proof of Theorem 1. *Necessity.* The necessity of (C_2) was proven in the remarks preceding the statement of the theorem.

Sufficiency. Let $w = \{w_k\}$ be a bounded sequence ($|w_k| \leqq 1$ for all k) that we wish to interpolate at the points $\{z_k\}$. The function

$$h_n(z) = \sum_{k=1}^n w_k B_{nk}(z)/b_{nk}$$

solves the problem at the first n points. We rewrite this

$$h_n(z) = B_n(z) \sum_1^n (w_k/b_{nk})(1-\bar{z}_k z)/(z-z_k).$$

Therefore the function

$$B_n(z)\{\sum_1^n (w/b_{nk})(1-\bar{z}_k z)/(z-z_k) - g(z)\}$$

will also solve the problem, for any $g \in H_\infty$. We wish to choose g so as to minimize the norm in H_∞. Let

$$(6) \qquad m_n(w) = \inf_{g \in H_\infty} \| B_n(z)\{\sum (w_k/b_{nk})(1-\bar{z}_k z)/(z-z_k) - g(z) \| \|_{H_\infty}.$$

We must show that $m_n(w)$ is uniformly bounded in n and w (w in the unit ball of l_∞). Let us take (6) onto the boundary of the unit circle, and let ϕ denote the rational function given by the summation. Since $|B_n(e^{i\theta})| = 1$ we have

$$m_n(w) = \inf_g \| \phi - g \|_{L_\infty} \qquad (g \in H_\infty).$$

We now apply the duality relation (2), with $E = L_1$, $F = H_1$, $E^* = L_\infty$, $F^\perp = H_\infty$. We obtain

$$m_n(w) = \sup_f |(f, \phi)| \qquad (f \in H_1, \| f \|_1 = 1).$$

Evaluating (f, ϕ) by (1) we have

$$(7) \qquad m_n(w) = \sup_f |\sum_1^n (w_k/b_{nk}) f(z_k)(1-|z_k|^2)|.$$

Since $\delta \leqq |b_{nk}| \leqq 1$ for all n, k we have

$$(8) \qquad \begin{aligned} &\sup_f \sum_1^\infty |f(z_k)|(1-|z_k|^2) \\ &\qquad \leqq \sup_n \sup_w m_n(w) \leqq \delta^{-1} \sup_f \sum_1^\infty |f(z_k)|(1-|z_k|^2), \end{aligned}$$

where $f \in H_1$, $\| f \|_1 = 1$, and w beolngs to the unit ball of l_∞.

Now if $f \in H_1$ has no zeros in the unit circle, then $f = g^2$ with $g \in H_2$. If f has zeros, then $f = Bf_1$, where B is a Blaschke product, f_1 has no zeros, $\| f \| = \| f_1 \|$, and $|f(z_k)| < |f_1(z_k)|$ for all k. Therefore the supremum on the right side of (8) is equal to

$$(9) \qquad \sup_g \sum |g(z_k)|^2 (1-|z_k|^2) \qquad (g \in H_2, \| g \|_2 = 1).$$

We now show that the finiteness of (9) is equivalent to a weighted interpolation problem in H_2

Lemma 1. *Let $\{z_n\}$ satisfy condition* (C_1) *of Theorem* 1. *Then the following two statements are equivalent:*

$$\sum |g(z_k)|^2 (1-|z_k|^2) \leqq M \, \|g\|^2 \tag{10}$$

for some constant M and all $g \in H_2$;

(11) *there is a constant m such that if $\{w_k\}$ is any square summable sequence, then there is a $g \in H_2$ with*

$$\|g\|^2 \leqq m \sum |w_k|^2 \text{ and } g(z_k)(1-|z_k|^2)^{\frac{1}{2}} = w_k \qquad (k=1,2,\cdots).$$

We shall show in fact that if (10) holds, then the constant m in (11) can be taken to be $(1/\delta^2)M$, while if (11) holds, then the constant M in (10) can be taken to be m.

Proof. The proof is similar to the proof given at the beginning of the sufficiency part of Theorem 1. Let $w = \{w_k\}$ be a sequence for which $\sum |w_k|^2 \leqq 1$. We wish to show that the problem of interpolating all such w in a uniformly bounded manner in H_2 (i.e. (11)) is equivalent to (10). Let

$$h_n(z) = \sum_1^n w_k B_{nk}(z)/b_{nk}(1-|z_k|^2)^{\frac{1}{2}}.$$

Then $h_n(z_k)(1-|z_k|^2)^{\frac{1}{2}} = w_k$ $(k=1,2,\cdots,n)$.

As before we modify h_n and arrive at (6), except that now $g \in H_2$ and the norm is the H_2 norm. The duality relation now leads to

$$m_n(w) = \sup_f \left| \sum_1^n (w_k/b_{nk}) f(z_k)(1-|z_k|^2)^{\frac{1}{2}} \right| \qquad (\|f\|_2 = 1). \tag{7'}$$

The analogue of (8) with both sides squared is:

$$\begin{aligned}\sup_f \sum |f(z_k)|^2 (1-|z_k|^2) \\ \leqq [\sup_n \sup_w m_n(w)]^2 \leqq \delta^{-2} \sup_f \sum |f(z_k)|^2 (1-|z_k|^2),\end{aligned} \tag{8'}$$

where $f \in H_2$, $\|f\|_2 = 1$, and w is in the unit ball of l_2. The number $[\sup_n \sup_w m_n(w)]^2$ will serve as the number m in (11), and the result follows.

To complete the proof of Theorem 1 it is now sufficient to establish (11), with $N = 2(1/\delta^4)(1-2\log\delta)$. This will be done in two lemmas, the first of which occurs in Carleson's paper.

LEMMA 2. *If $\{z_k\}$ satisfies condition* (C_1), *then*

$$(12) \qquad \sum_{j=1}^{\infty} (1-|z_j|^2)(1-|z_k|^2)/|1-\bar{z}_j z_k|^2 \leqq 1-2\log\delta \qquad (k=1,2,\cdots).$$

Proof. The identity

$$|(z_k-z_j)/(1-\bar{z}_j z_k)|^2 = 1-(1-z_j|^2)(1-|z_k|^2)/|1-\bar{z}_j z_k|^2$$

together with the inequality $1-b \leqq \exp(-b)$ and a little calculation shows that the series in (12), summed over $j \neq k$, is $\leqq -2\log\delta$, and the result follows from this.

LEMMA 3. *If $\{z_k\}$ satisfies condition (C_1) and if $\{w_k\}$ is any square summable sequence, then there is a $g \in H_2$ for which*

$$\|g\|^2 \leqq (2/\delta^4)(1-2\log\delta)\sum|w_k|^2$$

and

$$g(z_k)(1-|z_k|^2)^{\frac{1}{2}} = w_k \qquad (k=1,2,\cdots).$$

Proof. For this proof (f,g) will denote the inner product in H_2:

$$(13) \qquad (f,g) = \frac{1}{2\pi}\int_0^{2\pi} f(e^{i\theta})\bar{g}(e^{i\theta})\,d\theta$$

(in contrast to (1)). Let

$$g_{nk}(z) = (B_n(z)/(z-z_k))^2(1-|z_k|^2)^{\frac{3}{2}}$$

and

$$f_n(z) = \sum_1^n w_k g_{nk}(z)/b_{nk}^2.$$

Then $f_n(z_k)(1-|z_k|^2)^{\frac{1}{2}} = w_k$ $(k=1,2,\cdots,n)$. Moreover,

$$(14) \qquad \|f_n\|^2 = (f_n,f_n) = \sum_{i,j=1}^{n} (w_i\bar{w}_j/(b_{ni}\bar{b}_{nj})^2)(g_i,g_j).$$

Here g_i stands for g_{n_i}. A calculation shows that

$$(g_i,g_j) = (1-|z_i|^2)^{\frac{3}{2}}(1-|z_j|^2)^{\frac{3}{2}}(1+z_i\bar{z}_j)/(1-z_i\bar{z}_j)^3.$$

Let $a_{ij} = (g_i,g_j)$. An easy calculation shows that $(1-|z_i|^2)^{\frac{1}{2}}(1-|z_j|^2)^{\frac{1}{2}} \leqq |1-\bar{z}_i z_j|$ for all i,j. Then by Lemma 2 we have:

$$\sum_j |a_{ij}| < 2\sum_j (1-|z_i|^2)(1-|z_j|^2)/|1-\bar{z}_i z_j|^2 \leqq 2(1-2\log\delta).$$

Since $a_{ji} = \bar{a}_{ij}$, the same bound holds for the sum on i. Therefore by (4) we have $\|f\|^2 \leqq (2/\delta^4)(1-2\log\delta)\sum|w_k|^2$, and the result follows.

This completes the proof of Theorem 1.

Remark 1. Condition (C_2) is conformally invariant and so Theorem 1 may be carried over to any simply connected domain. Thus in the strip $|y| < \sigma$ the points $z_k = k\pi$ satisfy condition (C_2) with the functions $f_k(z) = \sin(z - k\pi)/(z - k\pi)$. Here $1/\delta = \sup_k \sup_z |f_k(z)| = (e^{\sigma} - e^{-\sigma})/2\sigma$.

Remark 2. The functions f_n that were used in the proof of Lemma 3 are not the functions of minimal H_2 norm that solve the interpolation problem. It is a curious fact that if one uses the functions that must be minimal (their form is known, for example, from [13] Theorem 16), then one is led to a quadratic form that is much more difficult to handle than the one in (14). This form will be considered in the corollary to Theorem 3.

3. Interpolation by functions of class H_p.

Let the sequence $\{z_n\}$ be given and let (s) denote the set of all sequences of complex numbers. For each p $(1 \leqq p \leqq \infty)$ define a mapping $T_p\colon H_p \to (s)$ by:

$$T_pf = (f(z_1)(1 - |z_1|^2)^{1/p}, f(z_2)(1 - |z_2|^2)^{1/p}, \cdots).$$

THEOREM 2. *For each p $(1 \leqq p \leqq \infty)$ the necessary and sufficient condition on $\{z_n\}$ in order that $T_pH_p = l_p$ is that $\{z_n\}$ satisfy condition* (C_1), *or equivalently,*

$(C_{2,p})$ *there exist functions $f_k \in H_p$ such that*

(i) $f_k(z_i)(1 - |z_i|^2)^{1/p} = \delta_{ik}$

(ii) $\| f_k \|_p \leqq 1/\delta$.

The proof is very similar to that of Theorem 1 and so we shall merely sketch it. First, the equivalence of (C_1) and $(C_{2,p})$ is proven as before, using also the fact that $|f(z)| \leqq \| f \|_p/(1 - |z|^2)^{1/p}$ for all $f \in H_p$ (see [8], p. 304).

One uses the closed graph theorem to show that if $l_p \subset T_pH_p$, then the interpolation can actually be done with uniformly bounded H_p norms. (If N is the subspace of functions vanishing on $\{z_n\}$, then a mapping is defined from l_p into H_p/N. This map has a closed graph.) This implies the necessity of $(C_{2,p})$.

It is easy to see that if $T_pH_p \subset l_p$, then T_p has a closed graph and is therefore a bounded operator (this was obvious for $p = \infty$).

LEMMA 4. *Let condition (C_1) be satisfied. Then $T_pH_p \subset l_p$ for a given value of p if and only if $l_q \subset T_qH_q$ for the conjugate index q $(1/p + 1/q = 1)$.*

The proof is similar to the proof of Lemma 1.

To complete the proof of Theorem 2 one proceds as before (going from (8) to (9)) to show that $T_pH_p \subset l_p$ if and only if $T_2H_2 \subset l_2$, which reduces the problem to Lemma 3. QED

Remark 3. In H_1 an interpolating function can be given explicitly. Let $\{w_k\}$ be the values to be interpolated, with $\sum |w_k| (1 - |z_k|^2) < \infty$. Then

$$f(z) = \sum (B(z)/B'(z_k)) \, [1/(z - z_k) - 1/(z - z_k^*)] w_k$$

will solve the problem. Here $B(z)$ denotes the Blaschke product formed from the z_k, and $z_k^* = 1/\bar{z}_k$. A simple calculation shows that the expression in square brackets has norm 1 in H_1 (since $|z - z_k| = |1 - \bar{z}_k z|$ on $|z| = 1$). Also, $\| B \| = 1$, and so under condition (C_1) we have an absolutely convergent series of unit vectors in H_1.

4. Interpolation in Hilbert spaces of analytic functions. The results in Section 2 on interpolation in the space H_2 suggest similar problems for other Hilbert spaces of analytic functions. By a Hilbert space H of analytic functions we mean a Hilbert space whose elements are analytic functions in a domain D, and in which evaluation at a point is a continuous linear functional on H. This means that to each point $\zeta \in D$ there corresponds a unique function $K_\zeta(z) \in H$ (the kernel function) such that

$$f(\zeta) = (f, K_\zeta) \tag{15}$$

for all $f \in H$. Thus for $\| f \| \leqq 1$ we have

$$|f(\zeta)| \leqq \| K_\zeta \| = (K_\zeta, K_\zeta)^{\frac{1}{2}} = (K_\zeta(\zeta))^{\frac{1}{2}}. \tag{16}$$

Equality is attained for $f = K_\zeta / \| K_\zeta \|$. It follows easily from (15) that $K_a(b) = \overline{K_b(a)}$ for all $a, b \in D$. Indeed, $K_a(b) = (K_a, K_b)$, $K_b(a) = (K_b, K_a)$, and these are conjugates of one another. For a general discussion of kernel functions and their properties see Aronszajn (*Proceedings of the Cambridge Philosophical Society*, vol. 39 (1943) and *Transactions of the American Mathematical Society*, vol. 68 (1950)).

We note the following examples.

I. H_2. Here $K_\zeta(z) = 1/(1 - \bar{\zeta} z)$.

II. A_2. This is the space of functions $f(z) = \sum a_n z^n$, analytic for $|z| < 1$, with norm

$$\| f \|^2 = \frac{1}{\pi} \int\int_{|z|<1} |f(z)|^2 \, dx dy = \sum |a_n|^2/(n+1) < \infty.$$

Here $K_\zeta(z) = 1/(1 - \bar{\zeta} z)^2$.

III. H_2'. This is the space of functions $f(z) = \sum a_n z^n$ that are derivatives of functions of class H_2, with norm

$$\| f \|^2 = \frac{1}{\pi} \int\int |f(z)|^2 (1 - |z|^2)\, dxdy = \sum |a_n|^2/(n+1)(n+2) < \infty.$$

Here $K_\zeta(z) = 2/(1-\bar{\zeta}z)^3$.

IV. D (finite Dirichlet integral). These are the functions $f(z) = \sum a_n z^n$ analytic for $|z| < 1$, with $f(0) = 0$, whose derivative is in A_2. The norm is given by

$$\| f \|^2 = \frac{1}{\pi} \int\int |f'(z)|^2\, dxdy = \sum n\, |a_n|^2,$$

and $K_\zeta(z) = \log\{1/(1-\bar{\zeta}z)\}$.

V. Functions of exponential type in the upper half plane with

$$\| f \|^2 = \sup_y \frac{1}{2\pi} \int_{-\infty}^{\infty} |f(x+iy)|^2\, dx < \infty.$$

Here $K_\zeta(z) = i/(z+\bar{\zeta})$. By a Paley-Wiener theorem these functions are Fourier transforms of functions in $L_2(0,\infty)$.

VI. Entire functions of exponential type $\leqq \beta$ that belong to L_2 on the real axis. Here the norm is given by

$$\| f \|^2 = \frac{1}{2\pi} \int_{-\infty}^{\infty} |f(x)|^2\, dx,$$

and $K_\zeta(z) = \{2 \sin \beta(z-\bar{\zeta})\}/(z-\bar{\zeta})$. By another Paley-Wiener theorem these functions are Fourier transforms of functions in $L_2(-\beta, \beta)$.

In this paper we consider only the first three of these spaces.

In H_2 we considered the problem of weighted interpolation: when will the sequence $\{z_n\}$ be such that $\{f(z_n)(1-|z_n|^2)^{\frac{1}{2}}\}$ $(f \in H_2)$ is the most general sequence in l_2? In terms of the kernel function $K_\zeta(z)$ this becomes the following problem: for which sequences $\{z_n\}$ does $\{f(z_n)/(K_n(z_n))^{\frac{1}{2}}\}$ $(f \in H)$ represent the most general element in l_2? (We have written K_n for K_{z_n}.) In this form the problem can be posed for any Hilbert space of analytic functions. There are really two questions involved here: first, is the sequence always in l_2 for evey $f \in H$, and second, is every l_2 sequence obtained in this manner? Both of these questions can be formulated in an abstract Hilbert space as follows (see Bari [2]).

Let $\{x_n\}$ be a sequence of elements in a Hilbert space H. We shall say that $\{x_n\}$ is a *Bessel sequence* with bound M if

$$\sum |(x, x_n)|^2 \leqq M \| x \|^2 \tag{17}$$

for all $x \in H$. (If one merely assumes the convergence of the series on the left side of (17) for all $x \in H$, then one has a linear mapping from H to l_2. This mapping is easily seen to have a closed graph, which implies the existence of the constant M.)

We shall say that $\{x_n\}$ is a *Riesz-Fischer sequence* with bound m if to each sequence $\{c_n\} \in l_2$ there corresponds at least one $x \in H$ for which

$$(x, x_n) = c_n \quad (n = 1, 2, \cdots) \text{ and } \| x \|^2 \leqq m \sum | c_n |^2. \tag{18}$$

Here also if one merely assumes the existence of $x \in H$ such that $(x, x_n) = c_n$ $(n = 1, 2, \cdots)$ for each square summable sequence $\{c_n\}$, then the existence of the constant m follows from the closed graph theorem. Indeed, if J is the subspace of H orthogonal to all the x_n, then one has a mapping from l_2 into H/J, and this mapping has a closed graph.

If H is a Hilbert space of analytic functions in a domain D, and if $\{z_n\}$ is a sequence of points in D, then we take for the sequence x_n the normalized kernel functions: $K_n(z)/\| K_n \|$, where $K_n(z) = K_{z_n}(z)$. The Bessel property then becomes the inequality

$$\sum | f(z_n) |^2 / K_n(z_n) \leqq M \| f \|^2 \qquad (f \in H),$$

while the Riesz-Fischer property is a statement about weighted interpolation: to each square-summable sequence $\{c_n\}$ there corresponds an $f \in H$ such that

$$f(z_n)/(K_n(z_n))^{\frac{1}{2}} = c_n \quad (n = 1, 2, \cdots), \quad \| f \|^2 \leqq m \sum | c_n |^2.$$

Nina Bari [2] shows that in an abstract Hilbert space these properties are equivalent to a number of other properties (her terminology is somewhat different from ours). We shall need only one such equivalence.

THEOREM 3. *Let $\{x_n\}$ be an infinite sequence of elements in a separable Hilbert space, and let A denote the inner product matrix $((x_i, x_j))$ $(i, j = 1, 2, \cdots)$. Then*

I. *$\{x_n\}$ is a Bessel sequence with bound M if and only if the matrix A is a bounded operator on l_2 with bound M.*

II. *$\{x_n\}$ is a Riesz-Fischer sequence with bound m if and only if the matrix A is bounded below on l_2 with bound m.*

The matrix A is said to be bounded below by m if $\| a \| \leqq m \| A_n a \|$ for all n-tuples $a = (a_1, a_2, \cdots, a_n)$ and all n. Here the norms are l_2 norms, and A_n is the $n \times n$ matrix (x_i, x_j) $(i, j = 1, 2, \cdots, n)$. This is equivalent to saying that $\| a \|^2 \leqq m (A_n a, a)$ for all n and a, and it is also equivalent to $\| A_n^{-1} \| \leqq m$ for all n.

Proof. I. Let $\{x_n\}$ be a Bessel sequence, let $\{c_n\} \in l_2$, let p be fixed, and let $y = c_1 x_1 + \cdots + c_p x_p$. On the one hand,

$$\| y \|^4 = | (y, y) |^2 = | \sum \bar{c}_n (y, x_n) |^2 \leqq \sum | c_n |^2 \sum | (y, x_n) |^2$$
$$\leqq M \; \| y \|^2 \sum | c_n |^2.$$

Dividing by $\| y \|^2$ we have: $\| y \|^2 \leqq M \sum | c_n |^2$. On the other hand,

$$\| y \|^2 = (y \cdot y) = \sum c_i \bar{c}_j (x_i, x_j). \tag{19}$$

Thus the quadratic form in (19) is bounded by M, which implies that the matrix A is bounded by M.

Conversely, let A be bounded by M and let $\{e_n\}$ be a complete orthonormal set in H. We first show that there is a bounded operator $T \colon H \to H$, such that $T e_n = x_n$.

Indeed, let $x_i = \sum b_{ni} e_n$, and let T be the infinite matrix (b_{ni}). Then $T^* T = A$, and so $\| T \|^2 = \| T^* \|^2 = \| A \| = M$ (T^* is the conjugate transpose of T). Also, $T e_n = x_n$.

We now establish the Bessel property. Let $x \in H$ be given. Then $(x, x_n) = (x, T e_n) = (T^* x, e_n)$, and so

$$\sum | (x, x_n) |^2 = \| T^* x \|^2 \leqq M \| x \|^2.$$

II. Let $\{x_n\}$ have the Riesz-Fischer property, let $a_1, \cdots, a_n$ be given, and let $y \in H$ be the element of minimal norm such that $(y, x_i) = a_i$ $(i = 1, \cdots, n)$. Then y lies in the subspace spanned by $x_1, \cdots, x_n$ and therefore $y = c_1 x_1 + \cdots + c_n x_n$. Let $y_1 \in H$ be such that $(y_1, x_i) = a_i$ $(i \leqq n)$, $(y_1, x_i) = 0$ $(i > n)$, and $\| y_1 \|^2 \leqq m \sum | a_i |^2$. Then

$$\| y \|^2 \leqq \| y_1 \|^2 \leqq m \| a \|^2.$$

Also,

$$\bar{a}_i = (x_i, y) = \sum \bar{c}_j (x_i, x_j),$$

or more concisely, $\bar{a} = A_n \bar{c}$. Therefore

$$m \| a \|^2 \geqq (y, y) = \sum_{i,j} c_i \bar{c}_j (x_i, x_j) = (A_n \bar{c}, \bar{c}) = (\bar{a}, A_n^{-1} \bar{a}),$$

and so $\| A_n^{-1} \| \leqq m$.

Conversely, assume that $\| A_n^{-1} \| \leqq m$, and let $\{a_n\} \in l_2$ be given. To show that $\{x_n\}$ is Riesz-Fischer it will be sufficient to produce a sequence y_n such that

$$(y_n, x_i) = a_i \quad (i = 1, \cdots, n) \text{ and } \| y_n \|^2 \leqq m \sum | a_i |^2,$$

for by weak compactness a subsequence of y_n will converge to an element x satisfying (18).

Let $y_n = c_1 x_1 + \cdots + c_n x_n$. We wish to choose $\{c_i\}$ such that $a_i = (y_n, x_i)$ $(i = 1, \cdots, n)$. Just as before this means that $\bar{a} = A_n \bar{c}$, or $\bar{c} = A_n^{-1} \bar{a}$. Also,

$$\begin{aligned} \| y_n \|^2 = (y_n, y_n) = \sum c_i \bar{c}_j (x_i, x_j) &= (A_n \bar{c}, \bar{c}) \\ &= (\bar{a}, A_n^{-1} \bar{a}) \leqq m \| \bar{a} \|^2 = m \| a \|^2. \end{aligned}$$

This completes the proof.

We give an application of this theorem to the H_2 interpolation problem considered in Lemmas 1 and 3, in the case of exponential approach to the boundary. In this case we obtain a better constant than is given by Lemmas 1 and 3.

COROLLARY. *If the points* $\{z_n\}$ *satisfy the condition*

$$1 - | z_{n+1} | \leqq \alpha (1 - | z_n |)$$

for all n *and some* α $(0 < \alpha < 1)$, *then*

$$\sum | f(z_n) |^2 (1 - | z_n |^2) \leqq 2((1 + \alpha^{\frac{1}{2}})/(1 - \alpha^{\frac{1}{2}})) \| f \|^2$$

for all $f \in H_2$.

In Newman [11] (Theorem 2) it is shown that

$$1/\delta \leqq \prod_{n=1}^{\infty} ((1 + \alpha^n)/(1 - \alpha^n)),$$

where δ is the constant of condition (C_1) in Theorem 1. It can be shown that equality is attained here if $z_n = 1 - \alpha^n$ $(n = 1, 2, \cdots)$.

Proof. Since the kernel function for the space H_2 (the Szego kernel) is $1/(1 - \bar{\zeta} z)$, the corollary will follow from Theorem 3 if we can show that the matrix $A = \{a_{mn}\}$, where

$$a_{nm} = (1 - | z_n |^2)^{\frac{1}{2}} (1 - | z_m |^2)^{\frac{1}{2}} / (1 - \bar{z}_n z_m) \tag{20}$$

bounded above by $2(1 + \alpha^{\frac{1}{2}})/(1 - \alpha^{\frac{1}{2}})$. To do this we apply (4).

It follows from the hypothesis that $1-|z_{n+p}|\leqq\alpha^p(1-|z_n|)$. Also, $|1-\bar z_n z_m|\geqq 1-|z_{\min(n,m)}|$. Therefore

$$\sum_{n=1}^{\infty}|a_{nm}|=\sum_{1}^{m}|a_{nm}|+\sum_{m+1}^{\infty}|a_{nm}|$$

$$\leqq 2\sum_{1}^{m}((1-|z_m|)/(1-|z_n|))^{\frac{1}{2}}+2\sum_{m+1}^{\infty}((1-|z_n|)/(1-|z_m|))^{\frac{1}{2}}$$

$$\leqq 2\sum_{1}^{m}\alpha^{(m-n)/2}+2\sum_{m+1}^{\infty}\alpha^{(n-m)/2}<2(1/(1-\alpha^{\frac{1}{2}})+\alpha^{\frac{1}{2}}/1-\alpha^{\frac{1}{2}}).$$

5. **Two special Hilbert spaces.** In this section we consider the spaces A_2 and H_2' (see Examples II and III of Section 4). We shall need the following result of Schur [14].

THEOREM (Schur). *Let $A=(a_{ij})$ and $B=(b_{ij})$ be two Hermitian, positive definite $n\times n$ matrices of complex numbers. Let α_1, α_2 be the smallest and largest eigen-values of A, and let $\beta_1=\inf b_{ii}$, $\beta_2=\sup b_{ii}$ $(i=1,\cdots,n)$. Then $C=(a_{ij}b_{ij})$ is positive definite and all eigen-values of C lie between $\alpha_1\beta_1$ and $\alpha_2\beta_2$.*

Since the smallest and largest eigen-values are respectively the infimum and supremum of $\|Cx\|$ for $\|x\|=1$, it follows that

$$\|C\|\leqq\beta_2\|A\| \text{ and } \|C^{-1}\|\leqq(1/\beta_1)\|A^{-1}\|.$$

Let $\{z_n\}$ be a sequence of points in the unit circle and let H be a Hilbert space of analytic functions in the unit circle with kernel function $K_\zeta(z)$. We consider the unit vectors $K_n(z)/\|K_n\|$. Using the reproducing property (15) of the kernel function the inner product matrix of Theorem 3 becomes $(K_j(z_i)/\|K_i\|\,\|K_j\|)$. In particular, in H_2, A_2, and H_2' the general element of this matrix is:

$$H_2\colon\ (\delta_i\delta_j)^{\frac{1}{2}}/(1-\bar z_i z_j), \tag{21}$$

$$A_2\colon\ \delta_i\delta_j/(1-\bar z_i z_j)^2, \tag{22}$$

$$H_2'\colon\ (\delta_i\delta_j)^{\frac{3}{2}}/(1-\bar z_i z_j)^3. \tag{23}$$

Here $\delta_i=1-|z_i|^2$.

Finally, we introduce the operator T that associates to each $f\in H$ the weighted sequence of values

$$Tf=(f(z_1)/\|K_1\|,f(z_2)/\|K_2\|,\cdots). \tag{24}$$

THEOREM 4. *Let $\{z_n\}$ be a sequence of points in the unit circle* *satisfying condition* (C_1) *of Theorem* 1, *and let* $\delta_n = 1 - |z_n|^2$. *Then* $TA_2 = TH_2' = l_2$. *More precisely,*

$$(25)\qquad \begin{aligned} &\sum |f(z_n)|^2 \delta_n^2 \leqq (1 - 2\log\delta)\,\|f\|^2 \quad (\textit{all } f \in A_2) \\ &\sum |f(z_n)|^2 \delta_n^3 \leqq 2(1 - 2\log\delta)\,\|f\|^2 \quad (\textit{all } f \in H_2'), \end{aligned}$$

and, to each square summable sequence $\{c_n\}$ *there corresponds an* $f \in A_2$ *and a* $g \in H_2'$ *such that*

$$f(z_n)\delta_n = g(z_n)\delta_n^{\frac{3}{2}} = c_n,$$

$$\|f\|^2 \leqq m \sum |c_n|^2, \qquad \|g\|^2 \leqq m \sum |c_n|^2.$$

Here the norms are taken respectively in A_2 and in H_2', and the number m ins the smallest admissible bound for the H_2 interpolation problem (by Lemma 3, $m \leqq (2/\delta^4)(1 - 2\log\delta)$).

Proof. It follows from (4) and Lemma 2 that the matrices (22) and (23) are each bounded by $(1 - 2\log\delta)$. Equations (25) now follow from Theorem 3.

Equations (26) follow from Schur's theorem and Theorem 3, since the elements in (22) and (23) are respectively the squares and the cubes of the elements in (21), and the diagonal elements are all equal to one. This completes the proof.

We shall need an analogue of Schwarz's lemma for the spaces A_2 and H_2'.

LEMMA 5. *Let* a, b *be two points in the unit circle and let*

$$d = (1 - |a|^2)(1 - |b|^2)/|1 - \bar{a}b|^2.$$

Then

$$|f(b)| \leqq (\|f\|/(1 - |b|^2))(|a - b|/|1 - \bar{a}b|)(1 + d)^{\frac{1}{2}}$$

for all $f \in A_2$ *for which* $f(a) = 0$. *Also*

$$|f(b)| \leqq (2\,\|f\|/(1 - |b|^2)^{\frac{3}{2}})(|a - b|/|1 - \bar{a}b|)(1 + d + d^3)^{\frac{1}{2}}$$

for all $f \in H_2'$ *for which* $f(a) = 0$. *Equality is possible in both cases.*

Proof. Let H denote either of the spaces A_2 or H_2', let $K_\zeta(z)$ be its kernel function and let J be the subspace of all functions vanishing at a. Then J is itself a Hilbert space of analytic functions with the kernel function

$$(27)\qquad \phi_\zeta(z) = K_\zeta(z) - cK_a(z),$$

where $c = K_\zeta(a)/K_a(a)$. Indeed, $\phi_\zeta(a) = 0$, so for each fixed ζ, $\phi_\zeta \in J$. Also, if $f \in J$, then

$$(f, \phi_\zeta) = f(\zeta) - \bar{c}f(a) = f(\zeta)$$

and so ϕ_ζ reproduces the values of all $f \in J$. But the kernel function is always unique, and so ϕ_ζ is it.

Therefore for $f \in J$ we have:

$$\begin{aligned} |f(b)|^2 = |(f, \phi_b)|^2 \leqq \|f\|^2(\phi_b, \phi_b) = \|f\|^2 \phi_b(b) \\ = \|f\|^2(K_b(b) - |K_a(b)|^2/K_a(a)). \end{aligned}$$

Substituting the specific kernel functions for A_2 and H_2' we obtain the lemma.

We shall say that a sequence of points $\{z_n\}$ in the unit circle is *weakly separated* if there is a constant $c > 0$ such that

$$|z_i - z_j| \geqq c \max(\delta_i, \delta_j) \tag{28}$$

for all i, j (that is, the distance between points is greater than a constant multiple of the distance to the boundary). It is easy to see that if the z_n all lie on one radius, then this is equivalent to exponential approach to the boundary: $\limsup \delta_{n+1}/\delta_n < 1$.

Weak separation is equivalent to the following condition:

$$|z_i - z_j| \geqq c_1 |1 - \bar{z}_i z_j| \tag{29}$$

for some constant $c_1 > 0$ and all i, j. Indeed, writing a, b for z_i, z_j, we have $1 - |a|^2 \leqq 2(1 - |a|) \leqq 2|1 - \bar{a}b|$, and so (29) implies (28).

Conversely, a little calculation shows that if $|a| \leqq |b| < 1$ and if $x = |a - b|/(1 - |a|^2)$, then

$$|a - b|/|1 - \bar{a}b| \geqq x/(1 + x).$$

Therefore, (28) implies (29).

We now show that weak separation is a necessary condition for weighted interpolation.

THEOREM 5. *Let H be either of the spaces A_2, H_2', and let T be the operator in equation* (24). *If $l_2 \subset TH$, then the points $\{z_n\}$ are weakly separated. Furthermore, if the $\{z_n\}$ are weakly separated, then $TH \subset l_2$. More precisely, if* (28) *holds and if $b = \min(c, 1)$, then*

$$\begin{aligned} &\sum |f(z_n)|^2 \delta_n^2 \leqq (2/b)^2 \|f\|^2 \qquad (\text{all } f \in A_2), \\ &\sum |f(z_n)|^2 \delta_n^3 \leqq 2(2/b)^2 \|f\|^2 \qquad (\text{all } f \in H_2'). \end{aligned} \tag{30}$$

Proof. If $l_2 \subset TH$, then there is a constant m such that each element in the unit ball of l_2 can be obtained by weighted interpolation from an $f \in H$

with $\| f \| \leqq m$ (see the beginning of the proof of Theorem 2). Therefore, if i, j are given ($i \neq j$), then there is an $f \in H$, $\| f \| \leqq m$, such that

$$f(z_i)/(K_i(z_i))^{\frac{1}{2}} = 1, \qquad f(z_j) = 0.$$

(We could require $f(z_n) = 0$ ($n \neq i$), but we shall only use the values of f at z_i, z_j.) Applying Lemma 5 with $a = z_i$, $b = z_j$ we have in A_2:

$$1/(1 - |z_i|^2) \leqq (m/(1 - |z_i|^2))(|z_i - z_j|/|1 - \bar{z}_i z_j|)(1 + d)^{\frac{1}{2}}.$$

Therefore

$$(31) \qquad |z_i - z_j|/|1 - \bar{z}_i z_j| \geqq \text{const} > 0,$$

and this is equivalent to weak separation. Starting with the space H_2' we obtain (31) (with a different constant) in exactly the same way.

We now turn to the second part of the theorem. The points $\{z_n\}$ are given to be weakly separated and we must establish (30).

Let $b = \min(c, 1)$. It follows from (28) that the circles C_i: $|z - z_i| \leqq \frac{1}{2} d\delta_i$ are disjoint and are contained inside the unit circle. Also, $|f(z)|^2$ is a subharmonic function and so

$$(32) \qquad |f(z_i)|^2 \delta_i^2 \leqq (2/b)^2 \frac{1}{\pi} \iint_{C_i} |f(z)|^2 \, dxdy$$

for all f analytic in the unit circle. If $f \in A_2$ we sum (32) on i and obtain the first equation of (30).

For $f \in H_2'$ we first multiply both sides of (32) by δ_i, and note the inequality: $1 - |z_i|^2 \leqq 2(1 - |z|^2)$ for $z \in C_i$. Indeed, the right side is smallest for $|z| = |z_i| + \frac{1}{2} d\delta_i \leqq |z_i| + \frac{1}{2}\delta_i$, and for this value the inequality may be verified. Now summing on i we obtain the second equation of (30). This completes the proof.

COROLLARY. *If the points $\{z_n\}$ all lie on one radius, then a necessary and sufficient condition for weighted interpolation ($l_2 \subset TH$) in either of the spaces A_2, H_2' is that the z_n approach the boundary exponentially. In this case, one has $l_2 = TH$.*

This follows at once from Theorems 4 and 5.

Remark 4. It can be shown that if $f \in H_2$ and $\phi(z) = 1/(1 - z)^{\frac{1}{2}}$ then $f_1 = \phi f \in A_2$, and $f_2 = \phi^2 f \in H_2'$. Hence if $f(z_n)\delta_n^{\frac{1}{2}} = c_n$, then $f_1(z_n)\delta_n = f_2(z_n)\delta_n^{\frac{3}{2}} = c_n$ ($n = 1, 2, \cdots$). Thus if one can solve the H_2 problem explicitly for the case when the points z_n all lie on one radius, then one also has an explicit solution of the problem in the spaces A_2 and H_2'.

Finally, we would like to discuss a result of Epstein, Greenstein, and Minker [4]. They consider the space H of functions analytic in the strip $D\colon |y| < \sigma$ for which the area norm is finite

$$\|f\|^2 = \int\int_D |f(z)|^2\,dxdy < \infty. \tag{33}$$

This is a Hilbert space with the kernel function

$$K_\zeta(z) = (\pi/16\sigma^2)\{\operatorname{sech}(\pi(z-\bar{\zeta})/4\sigma)\}^2.$$

They consider interpolation at the points $\{k\pi\}$ $(-\infty < k < \infty)$ and they show by Fourier analysis that the necessary and sufficient condition on a sequence $\{c_n\}$ that it be the set of values of an $f \in H$ at these points is that $\sum |c_n|^2 < \infty$. Since $K_x(x) = \text{const.}$ for x real, their problem can be considered as a problem in weighted interpolation.

To put the problem into our framework we consider the mapping

$$z = \phi(w) = \tanh(\pi w/4\sigma)$$

$(w \in D, |z| < 1)$ from the domain D to the unit circle. The points $w_n = n\pi$ go over into the points $z_n = \tanh(n\pi^2/4\sigma)$. These points lie on the real axis $(-1 < z_n < 1)$, and

$$1 - |z_n|^2 = \{\operatorname{sech}(n\pi^2/4\sigma)\}^2.$$

Thus $z_n \to 1$ exponentially as $n \to \infty$, and $z_n \to -1$ exponentially as $n \to -\infty$.

An application of Theorem 3 (just as in the corollary to Theorem 3) shows that

$$\sum_{-\infty}^{\infty} |f(z_n)|^2(1-|z_n|^2) \leqq (8\coth(\pi^2/8\sigma))\|f\|^2_{H_2}$$

for all $f \in H_2$. From Lemma 1, Remark 1, and Theorem 4 we obtain similar results for the values of functions in A_2 at these points. Finally, to go back to the space H in the strip it is necessary to "transplant" the functions of A_2 and multiply by the derivative of the mapping function. Thus, if $f \in A_2$, then

$$g(w) = f(\phi(w))\phi'(w)$$

is in H, and $g(w_n) = (\pi/4\sigma)f(z_n)(1-|z_n|^2)$.

The theorem of [4] follows from this, and one could obtain a bound for the norm of the minimal interpolating function. The method just presented will establish a similar theorem for certain sets of points $\{w_n\}$ that are not in arithmetic progression. Using the corollary to Theorem 5 one can obtain the following result.

THEOREM 6. *A sequence of real numbers* $\{w_n\}$ *has the property that* $TH = l_2$ *if and only if there is a number* d *such that for all* n, m *one has*

$$| w_n - w_m | \geqq d > 0.$$

Here T is the operator: $Tf = (f(w_1), f(w_2), \cdots)$, and H is the Hilbert space of (33).

NEW YORK UNIVERSITY,
UNIVERSITY OF MICHIGAN, NEW YORK UNIVERSITY.

REFERENCES.

[1] S. Banach, *Théorie des opérations linéaires*, Warszawa, 1932.

[2] N. Bari, "Biorthogonal systems and bases in Hilbert space," *Učeniye Zapiski, Moskovskiĭ Ordena Lenina Gosudarstvennyĭ Universitet imeni M. V. Lomonosova*, vol. 148, *Matematika*, 4 (1951), pp. 69-107 (Russian); *Mathematical Reviews*, vol. 14 (1953), p. 289.

[3] L. Carleson, "An interpolation problem for bounded analytic functions," *American Journal of Mathematics*, vol. 80 (1958), pp. 921-930.

[4] B. Epstein, D. Greenstein, J. Minker, "An extremal problem with infinitely many interpolation conditions," *Annales Academiae Scientiarum Fennicae, Series A, 250*, vol. 10 (1958), pp. 3-9.

[5] S. Ya. Havinson, "On some extremal problems of the theory of analytic functions," *Učeniye Zapiski, Moskovskiĭ Ordena Lenina Gosudarstvennyĭ Universitet imeni M. V. Lomonosova*, vol. 148, *Matematika*, 4 (1951), pp. 133-143 (Russian).

[6] W. Hayman, "Interpolation by bounded functions," *Université de Grenoble, Annales de l'Institut Fourier*, vol. XIII (1958), pp. 277-290.

[7] V. Kabaila, "On interpolation by functions of class H_δ," *Uspekhi Matematičeskih Nauk*, vol. 13, no. 1 (1958), pp. 181-188 (Russian).

[8] A. J. Macintyre, W. W. Rogosinski, "Extremum problems in the theory of analytic functions," *Acta Mathematica*, vol. 82 (1950), pp. 275-325.

[9] A. G. Naftalevitch, "On interpolation by functions of bounded characteristic," *Učeniye Zapiski, Vilnius Gos. Univ.*, V (1956), pp. 5-27 (Russian).

[10] R. Nevanlinna, "Über beschränkte analytische Funktionen," *Annales Acedemiae Scientiarum Fennicae*, vol. 32, Nr. 7 (1929), pp. 1-75.

[11] D. J. Newman, "Interpolation in H_∞," *Transactions of the American Mathematical Society*, vol. 92 (1959), pp. 501-507.

[12] I. I. Privaloff, *Randeigenschaften analytischer Funktionen*, Berlin, 1956 (Russian edition: Moscow, 1950).

[13] W. W. Rogosinski, H. S. Shapiro, "On certain extremum problems for analytic functions," *Acta Mathematica*, vol. 90 (1953), pp. 287-318.

[14] I. Schur, "Bemerkungen zur Theorie der beschränkten Bilinearformen mit unendlich vielen Veränderlichen," *Journal für die Reine und Angewandte Mathematik*, vol. 140 (1911), pp. 1-28.

[15] ———, Über Potenzreihen, die im Innern des Einheitskreises beschränkt sind," *ibid.*, vol. 147 (1917), pp. 205-232; vol. 148 (1918), pp. 122-145.

REPRESENTATION OF A SEMIGROUP BY TRANSFORMATIONS ACTING TRANSITIVELY ON A SET.*

By E. J. TULLY, JR.[1]

A *representation* of a semigroup S will mean here a homomorphism of S into the semigroup of all transformations of some set M into itself. This concept may be identified in an obvious way with that of a *set with semigroup of operators*, which will also be called an *operand* over a semigroup, symbolized by M_S. By this we mean a set M together with a semigroup S and a mapping $(x, a) \rightarrow xa$ of $M \times S$ into M, such that $(xa)b = x(ab)$ for all $x \in M$, $a, b \in S$.

The theory of representations (by transformations) of groups has been extensively studied; accounts of this theory are given in [2] and [4]. The corresponding theory for semigroups has been studied relatively little. Stoll [6] has studied the representations of finite simple semigroups. He has also introduced the concept of transitive system (which we shall call *strictly cyclic operand* or *strictly cyclic representation*). By this is meant an operand M_S such that $xS = M$ for some $x \in M$, where $xS = \{xa \colon a \in S\}$. Thurston [8] has studied the *congruence relations on an operand* M_S (i. e., equivalence relations σ on M such that $x\sigma y$ implies $xa\sigma ya$ for all $x, y \in M, a \in S$), calling them S-equivalences, and calling M an S-set.

The present paper determines those representations of a semigroup S which are strictly cyclic (thus generalizing [6]), and more particularly those which are *transitive* (i. e., in which $xS = M$ for all $x \in M$; not the same thing as transitive system in the sense of Stoll) or *0-transitive* (i. e., such that $|M| \geqq 2$ and $xS = M$ for all $x \in M$ except one x for which $xS = x$). In particular we shall obtain conditions for S to have *faithful* (i. e., 1-1) representations of the types considered.

Section 1 deals with strictly cyclic representations of a semigroup S. We show that all such representations arise (essentially) by letting S act by right multiplication on the set of σ-classes where σ is a right congruence on S such that $ea\sigma a$ (some $e \in S$, all $a \in S$) (1.1). The representation is faithful if and only if σ contains (i. e., is less fine than) no (2-sided) congruence except the identity relation (1.2). A necessary and sufficient condition for

---

* Received October 28, 1960.

[1] The writing of this paper was supported in part by the National Science Foundation. The author wishes to express gratitude to Professor A. H. Clifford for many valuable criticisms and suggestions.

the existence of a faithful strictly cyclic representation (1.3) is an immediate corollary; this condition is very weak since it is satisfied by any semigroup with identity (1.4).

Section 2 shows that all transitive representations arise by letting S act on the σ-classes where σ is a right congruence, $ea\sigma a$ (some $e \in S$, all $a \in S$) and each σ-class meets each right ideal (2.1). A *n.a.s.c.* for the existence of a faithful transitive representation follows immediately (2.2). Similar but more complicated conditions are obtained for 0-transitive representations. As applications of these results, we show among other things that a commutative semigroup S has a faithful transitive representation if and only if S is a group (2.4) and (in Section 4) that the free semigroup of rank n has such a representation if and only if $n \geqq 2$.

Section 3 studies [0-] transitive representations of semigroups with certain finiteness conditions (viz., the existence of a minimal right ideal for the case of transitive representations, and minimum condition on principal right ideals for the case of 0-transitive representations). The main result gives a *n.a.s.c.* not involving right congruence relations for the existence of a faithful [0-] transitive representation (3.4 and 3.4′).

Section 4 gives some examples.

Notation. Transformations will be written on the right. If A and B are sets, $A - B$ denotes $\{x \colon x \in A, x \notin B\}$. $|A|$ denotes the cardinal of A. $A \subseteq B$ means "A is a subset of B." $A \subset B$ means "A is a proper subset of B." $\mathcal{L}$, $\mathcal{R}$ and $\mathcal{H}$ are used in the sense of Green [3] to denote certain equivalence relations on a semigroup.

1. Strictly cyclic representations.

We say that two operands M_S and N_S over the same semigroup are *isomorphic* (and we write $M_S \cong N_S$) if there is a 1-1 correspondence π between M and N with $(xa)\pi = (x\pi)a$ for all $x \in M$, $a \in S$. We call an element u of M a *strict generator* if $uS = M$. Thus M_S is strictly cyclic if and only if M has a strict generator.

If σ is a congruence relation on M_S, we can let S act on the set M/σ of σ-classes by defining $X \circ a$ ($X \in M/\sigma, a \in S$) to be the (unique) σ-class containing $Xa = \{xa \colon x \in X\}$. This gives a new operand which we denote by M_S/σ.

If S is a semigroup, we denote by S_S the operand in which S acts on itself by right multiplication. It is clear that the congruences on the operand S_S are precisely the right congruences on the semigroup S. Thus if σ is a right congruence on the semigroup, we can form the operand S_S/σ.

We call $e \in S$ a left identity modulo a right congruence σ if $ea\sigma a$ for all $a \in S$.

The following is the generalization to semigroups of the basic theorem on transitive representations of groups.

PROPOSITION 1.1. *Let u be a strict generator of M_S. Define a relation σ on S by: $a\sigma b$ if and only if $ua = ub$. Then σ is a right congruence, there is a left identity modulo σ, and $M_S \cong S_S/\sigma$.*

Proof. Suppose $a\sigma b$. Then $ua = ub$. Therefore $uac = ubc$ for all $c \in S$. This means that $ac\sigma bc$, so that σ is a right congruence. Let e be any solution of $ue = u$ (which exists because u is a strict generator). Then for $a \in S$, $uea = ua$ so that $ea\sigma a$. This shows that e is a left identity modulo σ. Now define a 1-1 mapping π of M onto S/σ by: $x\pi = \{a : ua = x\}$. Then it is easy to see that $(xa)\pi = (x\pi)a$, so that π is an isomorphism.

Note. Conversely, it is easy to see that if σ is a right congruence on S and there is a left identity modulo σ, then S_S/σ is strictly cyclic (each σ-class which contains a left identity modulo σ being a strict generator of S/σ).

We define the *kernel-congruence* κ of an operand M_S by: $a\kappa b$ if and only if $xa = xb$ for all $x \in M$. κ is a congruence on S. κ is the identity relation if and only if M_S is faithful.

PROPOSITION 1.2. *Let σ be a right congruence on a semigroup S, e a left identity modulo σ, κ the kernel-congruence determined by the operand S_S/σ. Then $a\kappa b$ if and only if $ca\sigma cb$ for all $c \in S$. Moreover κ is the largest left congruence (and therefore the largest 2-sided congruence) contained in σ. In particular, S_S/σ is faithful if and only if there is no left (equivalently, no 2-sided) congruence contained in σ except the identity relation. This is equivalent to the condition that $a = b$ whenever for all $c \in S$ $ca\sigma cb$.*

Proof. If $a\kappa b$, then $\Sigma \circ a = \Sigma \circ b$ ($\circ$ denoting the operation in S_S/σ) where Σ is any σ-class. This means that $ca\sigma cb$ for all $c \in S$, and the reasoning is reversible. Next we show that κ is contained in σ. Assume $a\kappa b$. Then $ea\sigma eb$, whence $a\sigma b$. Now suppose τ is any left congruence contained in σ. Then $a\tau b$ implies $ca\tau cb$ for all $c \in S$, so that $ca\sigma cb$. Hence $a\kappa b$. This shows that τ is contained in κ. The rest of the proposition is then clear.

COROLLARY 1.3. *A necessary and sufficient condition for a semigroup S to have a strictly cyclic faithful representation is that there exist a right congruence σ on S, such that there is a left identity modulo σ, and such that σ contains no left congruence except the identity relation.*

COROLLARY 1.4. *A sufficient condition for S to have a faithful strictly cyclic representation is that S have a left identity (and in this case S_S is strictly cyclic). If S is commutative then this condition is also necessary.*

2. Transitive representations of arbitrary semigroups. We call $X \subseteq M$ *invariant* if $XS \subseteq X$, where $XS = \{xa: x \in X, a \in S\}$. Thus, for M_S to be transitive (which means that each element of M is a strict generator) is equivalent to the assertion that the only invariant subsets of M are M and $\emptyset$. For M_S to be 0-transitive means that M contains an invariant element z and every $x \in M$ with $x \neq z$ is a strict generator. Let us call M_S the null operand of cardinal 2 if $|M| = 2$, $|MS| = 1$. Then it is easy to see that the following conditions are equivalent:

(1) M_S is either 0-transitive or the null operand of cardinal 2

(2) M has an invariant element z, and has no invariant subsets except M, $\{z\}$ and $\emptyset$.

We call M_S *primitive* if the only congruences on M are the identity relation and the universal relation. It is not difficult to show that if $|M| \geqq 3$ and M is primitive, then M is either transitive or 0-transitive.

Examples. Let M be any set. If S consists of all transformations on M, M_S is primitive and transitive. If $|M| \geqq 3$ and $S' = \{a \in S: |Ma| = 1\}$, then $M_{S'}$ is transitive but not primitive. If $|M| \geqq 2$, $z \in M$ and $T = \{a \in S: za = z\}$, M_T is primitive and 0-transitive. If $|M| \geqq 3$, $z \in M$ and $T' = \{a \in T: |(M - \{z\})S| = 1$, then $M_{T'}$ is 0-transitive but not primitive. Let M_S be any operand. Let $x \in M$, $X = xS \cup \{x\}$. Define σ on X_S by: $w\sigma y$ if and only if $w = y$ or $w, y \in Z = \{z \in X: x \notin zS\}$. Then X_S/σ is transitive or 0-transitive, according as $Z = \emptyset$ or $Z \neq \emptyset$.

PROPOSITION 2.1. *Let σ be a right congruence on S. The following are equivalent:*

(3) *S_S/σ is transitive*

(4) *For all $a, b \in S$ there exists $c \in S$ with $ac\sigma b$*

(5) *Each σ-class meets each right ideal of S.*

PROPOSITION 2.1′. *Let σ be as in 2.1. The following are equivalent:*

(6) *S_S/σ is 0-transitive or the null operand of cardinal 2*

(7) *One σ-class $R \neq S$ is a right ideal, and for all $a \in S - R$, $b \in S$ there exists $c \in S$ such that $ac\sigma b$*

(8) *One σ-class $R \neq S$ is a right ideal, and every σ-class meets every right ideal which is not contained in R.*

Proof. First note that for a σ-class A to be a strict generator of S/σ means that for all $a \in A$, $b \in S$ there exists $c \in S$ with $ac\sigma b$, or equivalently that every right ideal which meets A meets every σ-class. Hence (4) and (5) each assert that every σ-class is a strict generator, and this is equivalent to (3). For 2.1′, note that a σ-class A is an invariant element of S/σ if and only if A is a right ideal. Thus (7) and (8) each assert that $|M| \geqq 2$, that R is an invariant element of S/σ, and that every element of S/σ other than R is a strict generator. This is equivalent to (6).

Note. Many results (like the preceding proposition) are stated in two forms (one for transitive, the other for 0-transitive, representations). Hereafter we shall prove only the primed proposition of each pair. The other may be proved by similar methods.

COROLLARY 2.2. *A necessary and sufficient condition for S to have a faithful transitive representation is that there exist a right congruence σ on S such that σ satisfies* (4) *and contains no left congruence* [*equivalently, no 2-sided congruence*] *except the identity relation and such that there is a left identity modulo σ.*

COROLLARY 2.2′. *A necessary and sufficient condition for S to have a faithful 0-transitive representation is that there exist a right congruence σ on S such that σ satisfies* (7) *and contains no left congruence* [*equivalently, no 2-sided congruence*] *except the identity relation and such that there is a left identity modulo σ and $|S/\sigma| \geqq 2$.*

Proof. Combine 1.1, 1.2 and 2.1′.

COROLLARY 2.3 [2.3′]. *A sufficient condition for S to have a faithful* [0-] *transitive representation is that S be right* [*zero*] *simple and have a left identity.* (*In this case S_S is* [0-] *transitive and faithful.*)

PROPOSITION 2.4 [2.4′]. *A necessary and sufficient condition for a commutative semigroup S to have a faithful* [0-] *transitive representation is that S be a group* [*to which a zero-element has been adjoined*].

Proof. Given a faithful 0-transitive representation, obtain σ by 2.2′. By commutativity σ is a 2-sided congruence. Hence, σ is the identity relation. Hence S contains an actual left identity, e, and is right 0-simple with 0-element z. Clearly, $S - \{z\}$ is an $\mathcal{H}$-class containing an idempotent (viz., e), and hence is a group, so that S is a group with zero. The converse follows from 2.3′.

3. Transitive representations of semigroups with finiteness conditions. If R is a right ideal in S, R_S denotes the operand in which S acts on R by ordinary right multiplication.

PROPOSITION 3.1 [3.1′]. *Let M_S be a* [0-] *transitive operand* [*with invariant element z*]. *Let R be a right ideal of S* [*such that $MR \neq \{z\}$*]. *Then $M_S \cong R_S/\sigma$ for some congruence σ on R_S.*

Proof. Let $u \in M$ be such that $uR \neq \{z\}$. Then u is a strict generator. Hence by 1.1 $M \cong S/\pi$ where π is given by: $a\pi b$ if and only if $ua = ub$. Let σ be π restricted to R. Define $\phi: S/\pi \to R_S/\sigma$ by $\Pi\phi = \Pi \cap R$, where Π is a π-class. Let $J = \{a \in S: ua = z\}$ be the (unique) π-class which is a right ideal. Then $R - J \neq \emptyset$. Hence by 2.1′ R meets every π-class. Hence ϕ is onto. It is then clear that ϕ is an isomorphism.

PROPOSITION 3.2 [3.2′]. *Let R be a [non-] minimal [principal] right ideal in S. Let σ be a congruence on S [such that all non-generators in R are contained in a single σ-class Σ]. Then R_S/σ is a [0-] transitive operand [having Σ as its (unique) invariant element].*

Proof. The set J of non-generators in R is the largest proper invariant subset of R_S. Thus R_S/σ has no invariant subsets between $\{\Sigma\}$ and the whole of R/σ, since Σ is the image of J under the natural mapping $R \to R/\sigma$. Clearly Σ is an invariant element of R/σ, so that R/σ is 0-transitive.

PROPOSITION 3.3 [3.3′]. *Let R and σ [and J] be as in 3.2 [3.2′]. Then the kernel-congruence κ of the operand R_S/σ is given by: $a\kappa b$ if and only if $ca\sigma cb$ for all $c \in R$. In particular R_S/σ is faithful if and only if for all $a, b \in S$ with $a \neq b$ there exists $c \in R$ with $ca \not\sigma cb$.*

Proof. Clear.

THEOREM 3.4. *Let R be a minimal right ideal in S. Then the following are equivalent:*

(9) *S has a faithful transitive representation*

(10) *$ca = cb$ for all $c \in R$ implies $a = b$*

(11) *$ca = cb$ for all $c \in K$ implies $a = b$, where K is the union of the minimal right ideals of S.*

Proof. (9) $\Rightarrow$ (10) : Let M_S be faithful and transitive. Then $M \cong R_S/\sigma$, where σ is as in 3.1. Hence (10) follows from the last part of 3.3.

(10) $\Rightarrow$ (11) : Clear, since $R \subseteq K$.

(11) $\Rightarrow$ (9) : R_S is transitive by 3.2 (with $\sigma =$ the identity relation). Suppose R_S is not faithful. Then there exist $a, b \in S$ with $a \neq b$ and $ca = cb$ for all $c \in R$. By semigroup theory $K = SR$. Hence for all $d \in K$, there exists $f \in R$, $g \in S$ with $da = gfa = gfb = db$. This contradicts (11).

THEOREM 3.4′. *Let S be a semigroup which satisfies the minimum condition on principal right ideals. Then S has a faithful 0-transitive representation if and only if there exists an $\mathfrak{R}$-class R of S, not a minimal right* *ideal, such that (for* $a, b \in S$*)* $a = b$ *whenever for all* $c \in R$ *either* $ca = cb$ *or* $ca, cb \notin R$.

Proof. First let M_S be faithful and transitive. By 1.1 $M \cong S/\sigma$ for some right congruence σ on S. By 2.1′ one σ-class Σ is a right ideal and $\Sigma \neq S$. Let R' be minimal in the class of all principal right ideals not contained in Σ. Let R be the $\mathcal{R}$-class consisting of all generators of R'. By 3.1′ $M \cong R'_S/\sigma$ for some congruence σ on R'_S. By 2.1′ $\Sigma \cap R' \neq \emptyset$. Hence if R' were a minimal right ideal Σ would contain R', contradicting the definition of R'. Moreover if $a \in (R' - R) - \Sigma$ then Σ would not contain the right ideal $aS \cup \{a\}$ contradicting the minimality of R'. Thus we can apply 3.3′, so that for all $a, b \in S$ with $a \neq b$ there exists $c \in R'$ with $ca \not\sigma cb$. Hence $ca \neq cb$. Moreover ca and cb are not both in Σ (since Σ is contained in a single σ-class). Thus we have shown that R satisfies the condition stated in the theorem. Conversely, suppose such an $\mathcal{R}$-class R exists. Let R' be the principal right ideal generated by R. Define σ on R' by: $a\sigma b$ if and only if either $a = b$ or $a, b \notin R$. By 3.2′ R'_S/σ is 0-transitive. By 3.3′ R'_S/σ is faithful. (Note that we used the minimum condition only for the proof of the necessity of the condition.)

4. Examples. We call S (right) transitive if S has a faithful transitive representation, and left transitive if S is anti-isomorphic to a transitive semigroup. It is clear that the results of Sections 2 and 3 concerning transitive semigroups can be applied to left transitive semigroups by interchanging "left" and "right."

By 2.4 any commutative semigroup which is not a group is neither left nor right transitive. Moreover if S has a right ideal R such that $ca = cb$ for all $a, b \in S$, $c \in R$ then (as an immediate consequence of 3.1 and 3.3) S is not transitive. In particular, a semigroup with a zero element is neither left nor right transitive. If S is completely simple in the sense of Rees [5] with structure matrix P then it is easy to show (by 3.4) that S is transitive if and only if P has two rows which are not left multiples of each other. 3.4 gives a rather explicit condition for any semigroup having a minimal right ideal to be transitive.

We now give examples not having minimal right ideals.

Example 1. The bicyclic semigroup, which consists of all pairs of nonnegative integers with multiplication given by:

$$(i, j)(k, l) = (i + k - \min(j, k), j + k - \min(j, k)),$$

is transitive on both sides. The relation σ, given by: $(i, j)\sigma(k, l)$ if and only if $j \neq l$, satisfies 1.3. (σ coincides with the relation $\mathcal{L}$ in the sense of Green [3].)

Example 2. Let S be a semigroup containing at least two elements, T any semigroup, and P the free product (either with or without an identity element adjoined) of S and T. Then P is transitive on both sides.

Proof. Choose a fixed $a \in S$. Let Q be the set of all elements of P of one of the following forms: t, where $t \in T$; st, where $a \neq s \notin S$, $t \in T$; $\prod_{i=1}^{n} at_i \prod_{i=n+1}^{m} s_i t_i$, where $s_{n+1} \neq a$, $m = 2n$, $s_i \in S$, $t_i \in T$. Now, given any $p \in P$, write p (uniquely) as a product of elements belonging alternately to S and to T. From the left of the sequence thus obtained, delete repeatedly elements of Q until this is no longer possible. Call the resulting (possibly empty) sequence the normalized form of p. Define a right congruence σ on P by: $p\sigma q$ if and only if p and q have the same normalized forms. Then it is easy to see that σ satisfies 2.2.

In particular, the free semigroup of rank $n \geqq 2$ is transitive on both sides. (Recall that by 2.4 the free semigroup of rank 1 is not transitive.)

Example 3. Let $S = \{a\}$, $T = \{b\}$. Let P be the free product (with or without an identity) of S and T. Then P is neither left nor right transitive.

Proof. For $i = a$ or b, let $(i, n) \in P$ denote the product in P of n elements, alternately a and b, the first one being i. Suppose P is (say) right transitive. Let σ be as in 2.2. By (5) the σ-class containing a meets the right ideal $\{(a, n) : n > 1\}$. Let p be the least integer with $a\sigma(a, p)$ and $p > 1$. Similarly let q be the least integer with $b\sigma(b, q)$ and $q > 1$. Case I: one of p, q (say p) is even. Here $ab\sigma(a, p)$ so that $p = 2$. Hence $a\sigma(a, n)$ for every n. The σ-class containing b must meet the right ideal $\{(a, n) : n \geqq 1\}$. Hence $a\sigma b$. Hence P consists of a single σ-class, contradicting 2.2. Case II: p and q are both odd. Here it is easy to see that for all $x \in P$ we have $xa\sigma x(a, 1 + (p-1)(q-1))$ and yet $a \neq (a, 1 + (p-)(q-1))$. This contradicts the last sentence of 1.2.

Example 4. Let M be an infinite set. Let S be the Baer-Levi semigroup (given in [1]), which consists of all 1-1 transformations of M into M such that $|M - M\pi| = |M|$. S is obviously right transitive. We shall show that S is also left transitive.

Proof. Order M by the first ordinal whose cardinal is $|M|$. Then for $N \subseteq M$, $|N| = |M|$, it follows that N (ordered by restriction) has the same ordinal as M. Hence there is a (unique) order isomorphism π_N of N onto M.

Given $\alpha \in S$, $\pi_{M\alpha}$ is a permutation of M. Define σ on S by: $\alpha\sigma\beta$ if and only if $\pi_{M\alpha} = \pi_{M\beta}$. It can be shown that σ is a left congruence, that each σ-class meets each left ideal, and that given $\alpha, \beta \in S$ with $\alpha \neq \beta$, there exists $\gamma \in S$ with $\alpha\gamma$ and $\beta\gamma$ in different σ-classes.

Example 5. The direct product of any number of transitive semigroups is transitive.

Example 6. Let S be a semigroup. Let $P = (p_{ij})$ be an $m \times n$ matrix of elements of S. Let T be the Rees matrix semigroup, which consists of all $n \times m$ matrices having an element of S in one place and zeros elsewhere, multiplication being defined by $A \circ B = APB$ for $A, B \in T$. This semigroup was considered in [7] and [5] for the case where S is a group.

Two rows, i and j, of P will be called dependent if, for some $a, b \in S$, $p_{ik}a = p_{jk}b$ for all k. Now if S is right transitive and no two rows of P are dependent, T is right transitive. (For, given σ on S as in 2.2, identify two elements $A = (a_{ij})$ and $B = (b_{ij})$ of P whenever for all i, j either $a_{ij} = b_{ij} = 0$ or $a_{ij}\sigma b_{ij}$. This gives a right congruence having the desired properties.) On the other hand, if two rows of P are dependent, then T is not right transitive.

CALIFORNIA INSTITUTE OF TECHNOLOGY.

REFERENCES.

[1] R. Baer and F. Levi, "Vollständige irreduzibele Systeme von Gruppenaxiomen," *Sitzungsberichte der Heidelberger Akademie der Wissenschaften, Mathematisch-naturwissenschaftliche Klasse, Beiträge zur Algebra*, No. 18 (1932), 12 pp.

[2] W. Burnside, *Theory of Groups of Finite Order*. 2nd ed. Cambridge Univ. Press, Cambridge, England, 1911. Reprinted by Dover Publications Inc., New York, 1955.

[3] J. A. Green, "On the structure of semigroups," *Annals of Mathematics*, vol. 54 (1951), pp. 163-172.

[4] M. Hall, *The Theory of Groups*. Macmillan, New York, 1959.

[5] D. Rees, "On semi-groups," *Proceedings of the Cambridge Philosophical Society*, vol. 36 (1940), pp. 387-400.

[6] R. R. Stoll, "Representations of finite simple semigroups," *Duke Mathematical Journal*, vol. 11 (1944), pp. 251-265.

[7] A. Suschkewitsch, "Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit," *Mathematische Annalen*, vol. 99 (1928), pp. 30-50.

[8] H. A. Thurston, "Equivalences and mappings," *Proceedings of the London Mathematical Society* (3), vol. 2 (1952), pp. 175-182.

ON DIFFERENTIALS IN FUNCTION FIELDS.*

By OSCAR ZARISKI[1] and PETER FALB.

Introduction. In order to develop a theory of differentials in algebraic functions fields K, of one variable, over *imperfect* ground fields k, and—above all—in order to prove in this case the classical formula which relates the order of dx at a place of K/k to the order of the different D_x at that place, Chevalley, in his book on Algebraic Functions of one variable, defines differentials by means of repartitions in K/k. The object of this paper is to show that also in the case of imperfect ground fields it is possible to develop the theory by using the conventional (formal) definition of a differential, without having recourse to repartitions. The advantage of our approach is that it enables one to deal with differentials $dx_1dx_2\cdots dx_r$ in function fields K/k of r independent variables (where repartitions are not available if $r>1$), by identifying (in an obvious sense) such a differential with the differential dx_1 in the field $K/k(x_2,\cdots,x_r)$ (if the characteristic p of k is different from zero, our new ground field $k'=k(x_2,\cdots,x_r)$ will not be perfect, even if the original ground field k was algebraically closed.).

Our proofs are essentially based on methods which have been developed by one of us in a paper on simple points (see Zariski [1]), and, in particular, on the mixed Jacobian criterion for simple points, established in that paper. As in that paper, so also here, we fix a model (normal curve) of K/k, we observe that any such model is already defined over $k^p(u_1,\cdots,u_\rho)$, where the u_i form a finite set of p-independent elements of k, and we deal with derivations with respect to the "p-parameters" u_i. This allows us to define the notion of "uniformizing coördinates" (which have been defined previously only for absolutely simple points) and to establish a crucial criterion for uniformizing coördinates (see § 1, Theorem 1). The notion of the order of a differential dx at a place p is defined by using uniformizing coördinates (see § 2, Definition 2). The role of Theorem 1 in the proof of the main result concerning the different (§ 3, Theorem 2) is that it allows us to reduce at once the proof of Theorem 2 to the case of cyclic Galois extensions, of prime

---

* Received May 10, 1961.

[1] This research was supported by the Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF 49(638)-494.

order. This cyclic case is treated in the last two sections of the paper, and here again the use of Theorem 1 is essential.†

We note that in the case of function fields K/k of r independent variables $x_1, \cdots, x_r$, where we take as new ground field the field $k(x_2, \cdots, x_r)$ (k-algebraically closed), the variables $x_2, \cdots, x_r$ play precisely the role of the p-parameters $u_1, \cdots, u_\rho$.

1. Uniformizing coordinates. Let V be an irreducible, r-dimensional affine variety, immersed in an affine space S_n and defined over a ground field k of characteristic $p \neq 0$. We assume that the function field K of V over k is a separable extension of k. Let $u_1, \cdots, u_\rho$ be a finite p-independent set of elements of k such that the ideal, $\mathfrak{I}(V)$, of V in $k\,[X_1, \cdots, X_n]$ has a basis $f_1(X), \cdots, f_N(X)$ of polynomials with coefficients in $k^p(u_1, \cdots, u_\rho)$; and let k_1 be a maximal subfield of k, containing k^p and such that $[k_1(u_1, \cdots, u_\rho) : k_1] = p^\rho$. We note that $k = k_1(u_1, \cdots, u_\rho)$. We will call $u_1, \cdots, u_\rho$ *p-parameters* of V/k, and k_1 a field of *p-constants* associated with the p-parameters $u_1, \cdots, u_\rho$. Any finite p-independent set U which contains a set U_0 of p-parameters of V/k is also a set of p-parameters of V/k, and if k_U is a field of p-constants associated with U, then we may take a suitable subfield of k_U as field of p-constants associated with U_0. This possibility of enlarging a set of p-parameters (and correspondingly shrinking the field of

---

† *Note added by O. Zariski in galley proofs.* During my visit to Frankfurt in June, 1961, Dr. Ernst Kuntz has called my attention to his most recent paper "Differentialformen inseparabler algebraischen Funktionenkörper" (*Math. Zeitschr.*, vol. 76 (1961), pp. 56-74) in which an essentially similar treatment of differentials over imperfect ground fields is found. In many respects the work of Dr. Kuntz goes farther than ours, namely (1) he does not assume that K/k is separable and (2) he deals also with function fields of varieties of arbitrary dimension (this latter generalization has also been carried out by Dr. Falb in his unpublished Harvard dissertation; in their presentation of the behaviour of differential forms on complete algebraic models of K/k, both Kuntz and Falb follows the procedure given by me in my lecture notes "Introduction to the theory of Algebraic Surfaces," Harvard University, 1957-1958). On the other hand, our characterization of uniformizing coördinates (Theorem 1) is not in Kuntz's paper. As this theorem plays an essential role in our paper, our treatment differs from that given by Kuntz in a significant way.

The paper of Kuntz is followed immediately, in the same issue of the *Mathematische Zeitschrift*, by a paper of Hans-Joachim Nastold, entited "Zum Dualitätssatz in inseparablen Funktionen = körpern der Dimension 1" (pp. 75-84). In this paper Dr. Nastold, using the work of Kuntz, proves the duality theorem for inseparable function fields K/k of dimension 1. Thus, on the basis of these two papers by Kuntz and Nastold, we have now, also for inseparable function fields, a complete formulation of the Riemann-Roch theorem, in which the differentials (or—equivalently—the canonical divisor class) appear in their conventional form (and not as repartitions).

p-constants) allows us to deal with the case of a finite set of varieties over k; i.e., there will then exist elements $u_1, \cdots, u_\rho$ and a field k_1 such that $\{u_1, \cdots, u_\rho\}$ is a set of p-parameters having k_1 as associated field of p-constants, for each variety of the set. For the moment, however, we shall assume that the p-parameters $u_1, \cdots, u_\rho$ and the field k_1 of p-constants have been fixed. As we shall consider derivations of K and of other fields or rings containing k, we stipulate now that *all derivations will be tacitly assumed to be trivial on* k_1 (but not necessarily on k).

Let W be an irreducible, s-dimensional subvariety of V/k, let $\mathfrak{O}$ be the local ring of W on V and let $\mathfrak{M}$ be the maximal ideal of $\mathfrak{O}$. We shall use the following notations:

$\mathcal{D}(K)$ = space of derivations of K (over k_1, by our convention);

$\mathcal{D}(W)$ = set of derivations D of K which are regular on W, i.e., such that $D\mathfrak{O} \subset \mathfrak{O}$;

$\mathcal{D}^*(W)$ = space of local W-derivations D^* on V, i.e., derivations D^* of $\mathfrak{O}$, with values in the residue field $k(W)$ of $\mathfrak{O}$;

$\bar{\mathcal{D}}(W)$ = space of derivations of $k(W)$.

$\mathcal{D}(K)$ and $\mathcal{D}(W)$ are vector spaces over K and $k(W)$ respectively, $\mathcal{D}(K)$ being of dimension $r+\rho$ (since K/k is separable and $[k : k_1] = p^\rho$); $\mathcal{D}(W)$ is an $\mathfrak{O}$-module while $\mathcal{D}^*(W)$ is (canonically) a $k(W)$-vector space ([1], p. 34). If W is simple on V, then $\dim \mathcal{D}^*(W) = r+\rho$ as a consequence of the Jacobian criterion for simple subvarieties ([1], p. 39). We have a mapping $D \rightarrow D^*$ of $\mathcal{D}(W)$ into $\mathcal{D}^*(W)$ given by $D^*z = \overline{Dz}$, $z \in \mathfrak{O}$ (where a bar above an element of $\mathfrak{O}$ denotes the $\mathfrak{M}$-residue of that element). Every element $\bar{D}$ of $\bar{\mathcal{D}}(W)$ can be lifted to an element $\bar{D}^*$ of $\mathcal{D}^*(W)$ by setting $\bar{D}^*z = \bar{D}\bar{z}$, $z \in \mathfrak{O}$. The mapping $\bar{D} \rightarrow \bar{D}^*$ is clearly an injection.

DEFINITION 1. *$\rho + r$ elements, $\xi_1, \cdots, \xi_{\rho+r}$, of $\mathfrak{O}$ are uniformizing coordinates of W if there exist $\rho + r$ derivations D_i of K, regular on W, such that $D_i\xi_j = \delta_{ij}$ $(i, j = 1, \cdots, \rho + r)$.*

PROPOSITION 1. *If W is simple on V, then there exist uniformizing coordinates of W.*

Proof. Let $x_i = \bar{X}_i = \mathfrak{J}(V)$-residue of X_i and let $\eta^1, \cdots, \eta_{\rho+n}$ stand for $u_1, \cdots, u_\rho, x_1, \cdots, x_n$ in some order (where $u_1, \cdots, u_\rho$ are the p-parameters). We may then assume that the Jacobian determinant

$$J(f_1, \cdots, f_{n-r}; \eta_{\rho+r+1}, \cdots, \eta_{\rho+n})$$

is not zero on W (i. e., is not an element of $\mathfrak{M}$), since the rank of the Jacobian matrix $J(f_1, \cdots, f_N; \eta_1, \cdots, \eta_{\rho+n})$ is $n-r$ ([1] p. 39). It follows that there exist $D_1, \cdots, D_{\rho+r}$ in $\mathcal{D}(K)$ such that $D_i\eta_j = \delta_{ij}$ $(i, j = 1, 2, \cdots, \rho + r)$ and that these derivations are uniquely determined. We have, for

$i = 1, \cdots, \rho + r; \nu = 1, \cdots, n - r$:

$$0 = D_i f_\nu = \frac{\partial f_\nu}{\partial \eta_i} + \sum_{\mu=1}^{n-r} \frac{\partial f_\nu}{\partial \eta_{\rho+r+\mu}} D_i \eta_{\rho+r+\mu}.$$

For fixed i, these equations, viewed as equations in the $D_i\eta_{\rho+r+\mu}$, have determinant which does not belong to $\mathfrak{M}$. Hence $D_i\eta_j \in \mathfrak{O}$ $(j = 1, \cdots, \rho + n)$. But $\mathfrak{O}$ is a quotient ring of $k_1[\eta_1, \cdots, \eta_{\rho+n}]$; therefore, the D_i are regular on W. Consequently $\eta_1, \cdots, \eta_{\rho+r}$ are uniformizing coordinates of W.

COROLLARY. *If W is simple on V, then $\mathcal{D}(W)$ is a free $\mathfrak{O}$-module of rank $\rho + r$, and if $\xi_1, \cdots, \xi_{\rho+r}$ are uniformizing coordinates of W and $D_1, \cdots, D_{\rho+r}$ are as in Definition* 1, *then the D_i form a free basis of $\mathcal{D}(W)$ over $\mathfrak{O}$. The mapping $D \rightarrow D^*$ of $\mathcal{D}(W)$ into $\mathcal{D}^*(W)$ given by $D^*z = \overline{Dz}$, $z \in \mathfrak{O}$, is a surjection, with kernel $\mathfrak{M}\mathcal{D}(W)$.*

Proof. It is clear that the derivations $D_1, \cdots, D_{\rho+r}$ of Definition 1 are linearly independent over $\mathfrak{O}$ and therefore form a basis of $\mathcal{D}(K)$ (over K). If $D \in \mathcal{D}(W)$, then $D = \sum \lambda_i D_i$, $\lambda_i \in K$, and since $\lambda_i = D\xi_i$, it follows that the λ_i are in $\mathfrak{O}$. Hence the D_i form a free $\mathfrak{O}$-basis of $\mathcal{D}(W)$. The second assertion follows from the fact that rank $\mathcal{D}(W)/\mathfrak{O} = \dim \mathcal{D}^*(W)/k(W)$ $(= \rho + r)$.

PROPOSITION 2. *Let $\eta_1, \cdots, \eta_{\rho+r}$ be uniformizing coordinates of W and let $D'_1, \cdots, D'_{\rho+r}$ be derivations of K, regular on W, such that $D'_i\eta_j = \delta_{ij}$. Then, given $\rho + r$ elements $\xi_1, \cdots, \xi_{\rho+r}$ in $\mathfrak{O}$, a necessary and sufficient condition that these elements be uniformizing coordinates of W is that the determinant $| D'_i\xi_j |$ does not belong to $\mathfrak{M}$.*

Proof. Assume that the ξ_i are uniformizing coordinates of W and let $D_1, \cdots, D_{\rho+r}$ be as in Definition 1. Since the D'_i form a basis of $\mathcal{D}(K)$ over K (actually a free $\mathfrak{O}$-base of $\mathcal{D}(W)$, by the previous corollary) we have $D_i = \sum_{j=1}^{\rho+r} \lambda_{ij} D'_j$ with $\lambda_{ij} \in K$ (in fact, $\lambda_{ij} \in \mathfrak{O}$), and $\lambda_{ij} = D_i\eta_j$. Applying D_i to ξ_q, we find that $\delta_{iq} = \sum_j (D_i\eta_j)(D'_j\xi_q)$, which shows that $\| D_i\eta_j \| \cdot \| D'_j\xi_q \|$ is the unit matrix. Since the determinant of each of these matrices is in $\mathfrak{O}$, each determinant is a unit in $\mathfrak{O}$.

Conversely, if $| D'_i\xi_j | \notin \mathfrak{M}$, then the matrix $\| D'_i\xi_j \|$ (whose entries are in $\mathfrak{O}$, as $D'_i \in \mathcal{D}(W)$, and $\xi_j \in \mathfrak{O}$) has an inverse $\| v_{ij} \|$, with $v_{ij} \in \mathfrak{O}$. Set $D_i = \sum_j v_{ij} D'_j$. Then $D_i \in \mathcal{D}(W)$ and $D_i \xi_j = \delta_{ij}$, from which it follows that the ξ_j are uniformizing coordinates of W.

In the proof of our next theorem, which characterizes uniformizing coordinates, we shall need a lemma concerning the function field of an arbitrary irreducible variety in S_n (over k) and in which *it is not assumed* that this function field is separable over k (as we later apply this lemma to the subvariety W of V).

LEMMA 1. *If an irreducible, s-dimensional variety W/k in S_n admits a field k_1 of p-constants and if $[k : k_1] = p^\rho$, then* $\dim \mathcal{D}(k(W)/k_1) \leqq s + \rho$, *and any set of generators of $k(W)$ over k_1 contains a subset of σ elements, $z_1, \cdots, z_\sigma$, where $\sigma = \dim \mathcal{D}(k(W)/k_1)$, such that $k(W)/k_1(z_1, \cdots, z_\sigma)$ is separable algebraic.*

Proof. By assumption, the ideal of W in $k[X_1, \cdots, X_n]$ has a basis $\{g_i(X_1, \cdots, X_n; u_1, \cdots, u_\rho);\ i = 1, 2, \cdots, N\}$ of polynomials with coefficients in $k^p[u_1, \cdots, u_\rho]$, where the u_i are p-parameters of W/k associated with the field k_1. Since W/k is simple on S_n, we know ([1] p. 39) that the mixed Jacobian matrix $J(g_1, \cdots, g_N; X_1, \cdots, X_n, u_1, \cdots, u_\rho)$ has rank $n - s$ on W (i.e., at a general point of W/k). If we denote by $Y_1, \cdots, Y_{n+\rho}$ the elements $X_1, \cdots, X_n, u_1, \cdots, u_\rho$ (in some order) and by $\xi_1, \cdots, \xi_{n+\rho}$ their $\mathfrak{J}(W)$-residues, then we may assume (say) that

$$\partial(g_1, \cdots, g_{n-s})/\partial(Y_{\rho+s+1}, \cdots, Y_{\rho+n}) \neq 0$$

at $(Y) = (\xi)$. This implies that $\xi_{\rho+s+1}, \cdots, \xi_{\rho+n}$ are separable algebraic over $k_1(\xi_1, \cdots, \xi_{\rho+s})$. As $k(W) = k_1(\xi_1, \cdots, \xi_{n+\rho})$, we have that $k(W)$ is separable algebraic over $k_1(\xi_1, \cdots, \xi_{\rho+s})$, and it is well-known ([2], Theorem 41, p. 127) that this implies that $\dim \mathcal{D}(k(W)/k_1) \leqq s + \rho$.

Let $\{y_\mu\}$ be a set of generators of $k(W)/k_1$ and set $L = k(W)$. Then every derivation of L/k_1 is trivial on $k_1(L^p)$, and L is a purely inseparable extension of $k_1(L^p)$, with $[L : k_1(L^p)] = p^\sigma$, $\sigma = \dim \mathcal{D}(L/k_1)$. We can extract from $\{y_\mu\}$ a set $\{y_1, \cdots, y_\sigma\}$ of elements such that

$$[k_1(L^p)(y_1, \cdots, y_\sigma) : k_1(L^p)] = p^\sigma,$$

and then we can construct σ linearly independent derivations $D_1, \cdots, D_\sigma$ of L/k_1 such that $D_i y_j = \delta_{ij}$ ([2] Corollary 5, p. 125). It is clear that any derivation of L over $k_1(y_1, \cdots, y_\sigma)$ vanishes on L. Therefore L is a separable algebraic extension of $k_1(y_1, \cdots, y_\sigma)$. This completes the proof of the lemma.

THEOREM 1. *Let W be an irreducible subvariety of V/k and let $\{u_1, \cdots, u_\rho\}$ and k_1 be p-parameters and associated field of p-constants for V/k. If W is simple on V/k, then, in order that given elements $\xi_1, \cdots, \xi_{\rho+r}$ of $\mathfrak{O}$ be uniformizing coordinates of W, it is necessary and sufficient that the following two conditions be satisfied:*

(i) *$k(W)$ is a separable algebraic extension of $k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+r})$, where $\bar{\xi}_i = \mathfrak{M}$-residue of ξ_i ($\mathfrak{O}$ is the local ring of W on V; $\mathfrak{M}$ is the maximal ideal of $\mathfrak{O}$);*

(ii) *$k_1[\xi_1, \cdots, \xi_{\rho+r}]$ contains a set of uniformizing parameters of W on V/k.*

Proof. Suppose that $\xi_1, \cdots, \xi_{\rho+r}$ are uniformizing coordinates of W. Let $\bar{D} \in \bar{\mathcal{D}}(W)$ and assume that $\bar{D} = 0$ on $k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+r})$. To establish (i) it will suffice to show that $\bar{D} = 0$. Let $\bar{D}^*$ be the local derivation of $\mathfrak{O}$ obtained by lifting $\bar{D}$ to $\mathcal{D}^*(W)$. It will suffice to show that $\bar{D}^* = 0$. Let $D_1, \cdots, D_{\rho+r}$ be as in Definition 1 and let $D^*_1, \cdots, D^*_{\rho+r}$ be the corresponding elements of $\mathcal{D}^*(W)$. Since $D^*_i\xi_j = \delta_{ij}$, the D^*_i are linearly independent over $k(W)$ and therefore form a basis of $\mathcal{D}^*(W)$ over $k(W)$. However, $\bar{D}^*\xi_j = 0$ for $j = 1, \cdots, \rho + r$ and $D^*_i\xi_j = \delta_{ij}$ $(i, j = 1, \cdots, \rho + r)$. It follows immediately that $\bar{D}^* = 0$.

We first prove (ii) under the additional assumption that $u_1, \cdots, u_\rho$ and k_1 are p-parameters and associated field of p-constants not only for V/k but also for W/k.

From (i) it follows that $\dim \mathcal{D}(k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+r}) = \dim \bar{\mathcal{D}}(W)$ (all derivations being assumed zero on k_1). Therefore, by Lemma 1,

$$\dim \mathcal{D}(k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+r})) \leqq \rho + s,$$

and thus, by known results on derivations of fields, it is possible to extract from $\{\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+r}\}$ a subset of $\rho + s$ elements, say $\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+s}$, such that $k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+r})$ is a separable algebraic extension of $k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+s})$ (compare with the proof of the second part of Lemma 1). Let $F_\lambda(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+s}, X)$ $(\lambda = 1, \cdots, r - s)$ be the minimal polynomial of $\bar{\xi}_{\rho+s+\lambda}$ over $k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+s})$; F_λ may be assumed to be a polynomial in $\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+s}$ (as well as in X). Let

$$(1) \qquad \tau_\lambda = F_\lambda(\xi_1, \cdots, \xi_{\rho+s}, \xi_{\rho+s+\lambda}), \qquad \lambda = 1, \cdots, r - s.$$

Then $\tau_\lambda \in \mathfrak{M} \cap k_1[\xi_1, \cdots, \xi_{\rho+r}]$, and in order to prove (ii) it will be sufficient to show that if there is a relation of the form $\sum a_\lambda \tau_\lambda \in \mathfrak{M}^2$, $a_\lambda \in \mathfrak{O}$, then the a_λ must belong to $\mathfrak{M}$ (since the τ_λ will then be uniformizing parameters of W on V, i.e., regular parameters of $\mathfrak{O}$). Now we have $D(\sum a_\lambda \tau_\lambda) \in \mathfrak{M}$ for any D in $\mathfrak{D}(W)$, and, in particular, for $\mu = 1, \cdots, r - s$,

$$D_{\rho+s+\mu}(\sum_\lambda a_\lambda \tau_\lambda) = \sum_\lambda (D_{\rho+s+\mu} a_\lambda) \tau_\lambda + \sum_\lambda a_\lambda (D_{\rho+s+\mu} \tau_\lambda) \in \mathfrak{M}.$$

Hence $\sum_\lambda a_\lambda (D_{\rho+s+\mu} \tau_\lambda) \in \mathfrak{M}$. But, by (1), we have $D_{\rho+s+\mu} \tau_\lambda = 0$ if $\mu \neq \lambda$ and $D_{\rho+s+\lambda} \tau_\lambda \notin \mathfrak{M}$ (since $\bar{\xi}_{\rho+s+\lambda}$ is separable algebraic over $k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+s})$ and therefore, $\frac{\partial F_\lambda}{\partial X} (\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+s}, \bar{\xi}_{\rho+s+\lambda}) \neq 0$). Thus $a_\lambda (D_{\rho+s+\lambda} \tau_\lambda) \in \mathfrak{M}$ and $a_\lambda \in \mathfrak{M}$. In the general case, we proceed as follows:

We fix in k_1 a finite set of p-independent elements $u_{\rho+1}, \cdots, u_\sigma$ such that the ideal $\mathfrak{J}(W)$ has a basis of polynomials with coefficients in $k^p(u_1, \cdots, u_\sigma)$. Then we fix a maximal subfield k_2 of k_1 such that

$$k^p < k_2, \ k_1 = k_2 (u_{\rho+1}, \cdots, u_\sigma) \ \text{ and } \ [k_1 : k_2] = p^{\sigma - \rho}.$$

Then it is clear that $u_1, \cdots, u_\sigma$ are p-parameters, and k_2 is an associated field of p-constants, for both V/k *and* W/k. We now use the notations of the proof of Proposition 1. The coefficients of $f_1, \cdots, f_{n-r}$ are in $k^p(u_1, \cdots, u_\rho)$, and $J(f_1, \cdots, f_{n-r}; \eta_{\rho+r+1}, \cdots, \eta_{\rho+n}) \notin \mathfrak{M}$. It follows from that proof, as applied to $u_1, \cdots, u_\sigma$ and k_2, that $\eta_1, \cdots, \eta_{\rho+r}, u_{\rho+1}, \cdots, u_\sigma$ are uniformizing coordinates of W relative to k_2. Let $D'_1, \cdots, D'_{\rho+r}, D'_{\rho+r+1}, \cdots, D'_{\sigma+r}$ be the corresponding derivations of $\mathfrak{O}$ (over k_2). We have therefore

$$D'_i \eta_j = \delta_{ij}, \qquad (i, j = 1, 2, \cdots, \rho + r),$$

and

$$D'_i u_\nu = 0, \qquad (i = 1, 2, \cdots, \rho + r; \nu = \rho + 1, \cdots, \sigma). \tag{2}$$

The relations (2) show that $D'_1, \cdots, D'_{\rho+r}$ are zero on k_1. Since both $\eta_1, \cdots, \eta_{\rho+r}$ and $\xi_1, \cdots, \xi_{\rho+r}$ are uniformizing coördinates of W, over k_1, we have, by Proposition 2, that the determinant of the derivatives $D'_i \xi_j$ $(i, j = 1, 2, \cdots, \rho + r)$ does not belong $\mathfrak{M}$. In view of (2), and since $D'_{\rho+r+\alpha} u_{\rho+\beta} = \delta_{\alpha\beta}$, it follows that also the $(\sigma + r)$-row determinant of the derivatives

$$D'_q \xi_j, \ D'_q u_{\rho+\beta} \quad (q = 1, 2, \cdots, \sigma + r; \ j = 1, 2, \cdots, \rho + r; \ \beta = 1, 2, \cdots, \sigma - \rho)$$

is not in $\mathfrak{M}$. Therefore, by Proposition 2, $\xi_1, \cdots, \xi_{\rho+r}, u_{\rho+1}, \cdots, u_\sigma$ are uniformizing coördinates of W, over k_2. Hence, by the preceding special case of the proof, the ring $k_2[\xi_1, \cdots, \xi_{\rho+r}, u_{\rho+1}, \cdots, u_\sigma]$ contains a set of uniformizing parameters of W on V/k. Since $k_2[u_{\rho+1}, \cdots, u_\sigma] = k_1$, the proof of (ii) is now complete.

Conversely, assume that $\xi_1, \cdots, \xi_{\rho+r}$ satisfy conditions (i) and (ii). Fix a set $\{\eta_1, \cdots, \eta_{\rho+r}\}$ of uniformizing coordinates of W (Proposition 1) and let $D'_1, \cdots, D'_{\rho+r}$ be as in Proposition 2. It will suffice to show that $| D'_i\xi_j | \notin \mathfrak{M}$. Suppose this is false. Then there exist elements $a_1, \cdots, a_{\rho+r}$ of $\mathfrak{O}$, *not all in* $\mathfrak{M}$, such that $\sum_i a_i(D'_i\xi_j) \in \mathfrak{M}$ $(j = 1, \cdots, \rho + r)$. Let, say, $a_1 \notin \mathfrak{M}$ and set $D = \sum_i a_i D'_i$. Then $D \in \mathfrak{D}(W)$ and $D\xi_j \in \mathfrak{M}$, from which it follows that $D\mathfrak{M} \subset \mathfrak{M}$ (by (ii)). Hence $\bar{D} = \mathrm{Tr}_W D$ is defined (by $\bar{D}\bar{z} = \overline{Dz}$, $z \in \mathfrak{O}$) and is an element of $\bar{\mathfrak{D}}(W)$. Since $\bar{D}\xi_j = 0$, we have $\bar{D} = 0$ (by (ii)), in contradiction with $\bar{D}\eta_1 = \bar{a}_1 \neq 0$. This completes the proof of the theorem.

COROLLARY. *If W is as in the Theorem 1, then there exist uniformizing coordinates $\eta_1, \cdots, \eta_{\rho+r}$ of W such that $\eta_1, \cdots, \eta_{r-s}$ (say) are uniformizing parameters of W on V.*

Proof. Let $\xi_1, \cdots, \xi_{\rho+r}$ be uniformizing coordinates of W (Proposition 1) and suppose that $k(W)$ is separable algebraic over $k_1(\bar{\xi}_1, \cdots, \bar{\xi}_{\rho+s})$ (compare with the second paragraph of the proof of the theorem). Let $t_1, \cdots, t_{r-s}$ be uniformizing parameters of W on V and set

$$\eta_1 = t_1, \cdots, \eta_{r-s}, = t_{r-s}, \ \eta_{r-s+1} = \xi_1, \cdots, \eta_{\rho+s} = \xi_{\rho+s}.$$

It is immediate from the theorem that the η_i are uniformizing coordinates of W on V.

We remark that all the results established in this section continue to hold (and are well-known) also in the case of characteristic zero. In this case, we have $k = k^p$, $\rho = 0$, and $k_1 = k$.

2. The order of a differential at a prime divisor. From now on we shall assume that $r = 1$. Let $\mathfrak{p}$ be a prime divisor of K/k and let $v = v_\mathfrak{p}$ be the valuation of K/k defined by $\mathfrak{p}$. Since for function fields of one variable the notion of a prime divisor is equivalent with that of an irreducible, 0-dimensional subvariety W of a normal (hence non-singular) model V of K/k, we can speak of uniformizing coordinates of $\mathfrak{p}$, relative to a given set of p-parameters $u_1, \cdots, u_\rho$ and an associated field k_1 of p-constants.

Since the space $\mathfrak{D}(K)$ of derivations of K (over k_1) has dimension $\rho + 1$, we may speak of differentials of K, of degree $\rho + 1$, and for any $\rho + 2$ elements

$A, z_1, \cdots, z_{\rho+1}$ of K, we have a differential $A dz_1, \cdots, dz_{\rho+1}$ of K. Furthermore, if $\xi_1, \cdots, \xi_{\rho+1}$ are uniformizing coordinates of $\mathfrak{p}$, then every $(\rho+1)$-fold differential of K can be written in the form $A d\xi_1 \cdots d\xi_{\rho+1}$, $A \in K$ (as an immediate consequence of the fact that the derivations $D_1, \cdots, D_{\rho+1}$ of Definition 1 form a basis of $\mathfrak{D}(K)$).

DEFINITION 2. *If x is a separating transcendental of K/k, if $\xi_1, \cdots, \xi_{\rho+1}$ are uniformizing coordinates of $\mathfrak{p}$, and if $dx du_1 \cdots du_\rho = A d\xi_1 \cdots d\xi_{\rho+1}$ (where the u_i are the given p-parameters), then the order of dx at $\mathfrak{p}$ (in symbols: $v(dx)$) is the integer $v(A)$.*

PROPOSITION 3. *The order of dx at $\mathfrak{p}$ is well-defined, i.e., $v(dx)$ is independent of the choice of the uniformizing coordinates ξ_i, of the p-parameters u_ν, and of the field k_1 of p-constants.*

Proof.

(a) That our definition of the order of dx is independent of the choice of the $\xi_i(u_1, \cdots, u_\rho$ and k_1 being fixed) follows immediately from Proposition 2.

(b) We next remark that it will suffice to prove the proposition for one particular separating transcendental x of K/k, which *we shall take as one of the generators* $x_1, \cdots, x_n$ of K/k. For if x' is another separating transcendental of K/k and if we set $dx' du_1 \cdots du_\rho = A' d\xi_1 \cdots d\xi_{\rho+1}$, then $A' = A D_x x'$, where D_x is the (unique) derivation of K over k such that $D_x x = 1$.

(c) We now demonstrate that for fixed $u_1, \cdots, u_\rho$ our definition is independent of the field k_1 of p-constants (we recall that k_1 is any maximal subfield of k, containing k^p, such that $[k_1(u_1, \cdots, u_\rho) : k_1] = p^\rho$, and is therefore not uniquely determined). We may, by (a), choose as uniformizing coordinates a suitable subset $\eta_1, \cdots, \eta_{\rho+1}$ of the set $\{\eta_1, \cdots, \eta_{\rho+n}\}$ of $\mathfrak{J}(V)$-residues of the elements $X_1, \cdots, X_n, u_1, \cdots, u_\rho$ (arranged in some order). We use here the notations of the proof of Proposition 1. Let $K_0 = k^p(\eta_1, \cdots, {}_{\rho+n})$. Then K_0 depends only on $u_1, \cdots, u_\rho$ (the generators $x_1, \cdots, x_n$ of K/k having been fixed; K_0 is in fact the function field of V over $k^p(u_1, \cdots, u_\rho)$). Let $D_1, \cdots, D_{\rho+1}$ be the derivations of K/k_1 such that $D_i \eta_j = \delta_{ij}$, $i, j = 1, \cdots, \rho+1$, and let $D^0{}_1, \cdots, D^0{}_{\rho+1}$ be their restrictions to K_0. The derivations $D^0{}_i$ of K_0 are independent of the choice of k_1 since they are uniquely determined by the conditions $D^0{}_i \eta_j = \delta_{ij}$ (compare with the proof of Proposition 1). Since $x \in K_0$ and since $A = \partial^0(x, u_1, \cdots, u_\rho)/\partial^0(\eta_1, \cdots, \eta_{\rho+1})$ (where the right hand side denotes the Jacobian determinant relative to the derivations $D^0{}_1, \cdots, D^0{}_{\rho+1}$), our assertion that, for given p-parameters $u_1, \cdots, u_\rho$, the order of dx is independent of the choice of k_1 is proved.

(d) We next remark that if $w_1, \cdots, w_\rho$ are p-parameters such that $k^p(w_1, \cdots, w_\rho) = k^p(u_1, \cdots, u_\rho)$, then $dx dw_1 \cdots dw_\rho = c\, dx du_1 \cdots du_\rho$, where $c \in k^p(u_1, \cdots, u_\rho)$, $c \neq 0$. For if $\delta_1, \cdots, \delta_\rho$ are the derivations of $k^p(u_1, \cdots, u_\rho)$ such that $\delta_i u_j = 0$ if $i \neq j$ and $\delta_i u_i = 1$, then c is equal to the Jacobian determinant $\partial(w_1, \cdots, w_\rho)/\partial(u_1, \cdots, u_\rho)$. It follows that $v(dx)$ is the same for two sets of p-parameters which generate the same field over k^p.

Let $\{u_1, \cdots, u_\rho\}$ and $\{w_1, \cdots, w_\tau\}$ be any two sets of p-parameters and let $[k^p(u_1, \cdots, u_\rho, w_1, \cdots, w_\tau) : k^p] = p^{\rho+\alpha} = p^{\tau+\beta} = p^\sigma$. We can enlarge the sets $\{u_1, \cdots, u_\rho\}$ and $\{w_1, \cdots, w_\tau\}$ to sets of p-parameters $\{u_1, \cdots, u_\sigma\}$ and $\{w_1, \cdots, w_\sigma\}$ such that $k^p(u_1, \cdots, u_\sigma) = k^p(w_1, \cdots, w_\sigma)$. Hence, in view of (d) the proof of our proposition will be complete if we show that the order of dx is unchanged when the set of p-parameters is enlarged.

Now let $\{u_1, \cdots, u_\rho\}$, $\{u_1, \cdots, u_\rho, u_{\rho+1}, \cdots, u_\sigma\}$, $\sigma > \rho$, be two sets of p-parameters one of which is contained in the other. Let k'_1 be a (fixed) field of p-constants associated with $\{u_1, \cdots, u_\sigma\}$. Then we can set, by (c), $k_1 = k'_1(u_{\rho+1}, \cdots, u_\sigma)$, so that $k'_1 \subset k_1$. We use the notations of the proof of Proposition 1. The coefficients of $f_1, \cdots, f_{n-r}$ are in $k^p(u_1, \cdots, u_\rho)$, and $J(f_1, \cdots, f_{n-r}; \eta_{\rho+r+1}, \cdots, \eta_{\rho+n}) \notin \mathfrak{M}$. It follows from that proof, applied to $u_1, \cdots, u_\sigma$ and k'_1, that $\eta_1, \cdots, \eta_{\rho+1}, u_{\rho+1}, \cdots, u_\sigma$ are uniformizing coordinates of $\mathfrak{p}$ relative to k'_1. If $D^0{}_{\rho+1}, \cdots, D^0{}_\sigma$ are the derivations of

$$k^p(\eta_1, \cdots, \eta_{\rho+n}, u_{\rho+1}, \cdots, u_\sigma)$$

such that $D^0{}_\alpha u_\beta = \delta_{\alpha\beta}$ $(\alpha, \beta = \rho + 1, \cdots, \sigma)$ and if

$$dx du_1 \cdots du_\sigma = B\, d\eta_1 \cdots d\eta_{\rho+1} du_{\rho+1} \cdots du_\sigma,$$

then

$$\begin{aligned} B &= \partial^0(x, u_1, \cdots, u_\sigma)/\partial^0(\eta_1, \cdots \eta_{\rho+1}, u_{\rho+1}, \cdots, u_\sigma) \\ &= \partial^0(x, u_1, \cdots, u_\rho)/\partial^0(\eta_1, \cdots, \eta_{\rho+1}) = A, \end{aligned}$$

and our assertion is proved.

3. The main result. Let K/k be a separably generated function field in one variable and let K' be a finite separable algebraic extension of K. In all that follows, we shall tacity assume that a set of p-parameters $u_1, \cdots, u_\rho$ of both K/k and K'/k (and similarly a field k_1 of p-constants of both K/k and K'/k) have been fixed in advance.[3] Let $\mathfrak{p}$ be a prime divisor of K/k;

---

[3] I. e., p-parameters of a normal model of K/k and of a normal model of K'/k.

let $\mathfrak{p}'$ be a prime divisor of K'/k lying over $\mathfrak{p}$; and let x be a separating transcendental of K over k (and hence also of K' over k). We denote by dx^K (respectively $dx^{K'}$) the differential dx viewed as a differential of K (respectively of K'). We shall use the following notations:

$(dx^K)_{\mathfrak{p}}$ = local $\mathfrak{p}$-component of the divisor of dx^K, i. e., $v_{\mathfrak{p}}(dx^K)\cdot\mathfrak{p}$;

$(dx^{K'})_{\mathfrak{p}'}$ = local $\mathfrak{p}'$-component of the divisor of $dx^{K'}$, i. e., $v_{\mathfrak{p}'}(dx^{K'})\cdot\mathfrak{p}'$;

$(dx^K)_{\mathfrak{p}'}$ = local $\mathfrak{p}'$-component of the extension of the divisor (dx^K) to K', i. e., $e_{\mathfrak{p}'/\mathfrak{p}}v_{\mathfrak{p}}(dx^K)\mathfrak{p}$, where $e_{\mathfrak{p}'/\mathfrak{p}}$ is the (reduced) ramification index of $\mathfrak{p}'$ over $\mathfrak{p}$;

$\mathfrak{O} = \mathfrak{O}_{\mathfrak{p}}$ = valuation ring of $\mathfrak{p}$;

$\mathfrak{O}' = \mathfrak{O}_{\mathfrak{p}'}$ = valuation ring of $\mathfrak{p}'$;

$\bar{\mathfrak{O}}$ = integral closure of $\mathfrak{O}$ in K'.

The main object of this paper is the proof of the following (well-known) theorem:

THEOREM 2. $(dx^{K'})_{\mathfrak{p}'} = (dx^K)_{\mathfrak{p}'} + (\mathfrak{D}_{\bar{\mathfrak{O}}/\mathfrak{O}})_{\mathfrak{p}'}$, *where* $(\mathfrak{D}_{\bar{\mathfrak{O}}/\mathfrak{O}})_{\mathfrak{p}'}$ *is the local* $\mathfrak{p}'$*-component of the divisor of the different* $\mathfrak{D}_{\mathfrak{O}/\mathfrak{O}}$ *of* $\bar{\mathfrak{O}}$ *over* $\mathfrak{O}$.

COROLLARY. *If* y *is a separating transcendental of* K/k *and if* $\mathfrak{r}$ *is a prime divisor of* K/k *such that* $v_{\mathfrak{r}}(y) \geqq 0$, *then* $v_{\mathfrak{r}}(dy) = v_{\mathfrak{r}}(\mathfrak{D}_{R/k[y]})$, *where* R *is the integral closure of* $k[y]$ *in* K.

In order to prove the corollary, we need only apply the theorem to the two fields $k(y)$ and K and note that the order of dy (viewed as a differential of $k(y)$) at any prime divisor of $k(y)$ which is not a pole of y, is equal to 0 (since $y, u_1, \cdots, u_\rho$ are obviously uniformizing coordinates of such a prime divisor, where $u_1, \cdots, u_\rho$ are the fixed p-parameters of K/k).

The proof of the theorem consists of a series of reductions, followed by a direct argument in two cases. In outline, the steps are:

(1) reduction to the case in which K'/K is a Galois extension; then, in the Galois case,

(2) reduction to the case in which K'/K is a cyclic extension of prime order;

(3) direct argument in the case of pure ramification

(4) direct argument in the case of purely inseparable residue field extension.

The remainder of the paper is divided into four sections which correspond to the steps in the proof.

Before we begin the proof, we remark that if $\mathfrak{p}'$ is unramified over $\mathfrak{p}$ (i. e., if $e_{\mathfrak{p}'/\mathfrak{p}} = 1$ and $k(\mathfrak{p}')$ is a separable algebraic extension of $k(\mathfrak{p})$), then Theorem 2 is true. In fact, in that case, if $\xi_1, \cdots, \xi_{\rho+1}$ are uniformizing coordinates of $\mathfrak{p}$, then, by Theorem 1, $\xi_1, \cdots, \xi_{\rho+1}$ are uniformizing coordinates of $\mathfrak{p}'$. Since $e_{\mathfrak{p}'/\mathfrak{p}} = 1$, we have, if $dx du_1 \cdots du_\rho = A d\xi_1 \cdots \xi_{\rho+1}$, that $v_{\mathfrak{p}'}(dx^K) = v_{\mathfrak{p}}(dx^K) = v_{\mathfrak{p}}(A) = v_{\mathfrak{p}'}(A) = v_{\mathfrak{p}'}(dx^{K'})$. However, ([2], p. 302, Theorem 28), $v_{\mathfrak{p}'}(\mathfrak{D}_{\bar{\mathfrak{O}}/\mathfrak{O}}) = 0$ and our assertion follows.

4. Reduction to the case in which *K′/K* is a Galois extension.

PROPOSITION 4. *Let K and K' be as in Theorem 2 and let K'' be a finite separable extension of K'. Then, if the theorem is true for any two of the extensions K'/K, K''/K, K''/K', the theorem is true for the third.*

Proof. Let $\mathfrak{O} = \mathfrak{O}_{\mathfrak{p}}$, $\mathfrak{O}' = \mathfrak{O}_{\mathfrak{p}'}$, $\mathfrak{O}'' = \mathfrak{O}_{\mathfrak{p}''}$ (where $\mathfrak{p}''$ is a prime divisor of K''/k lying over $\mathfrak{p}'$) and let $^{-}$, $^{=}$ denote integral closure in K', K'' respectively. Assume that the theorem holds for the extensions K'/K and K''/K. Then, we have:

$$(dx^{K''})_{\mathfrak{p}''} = (dx^K)_{\mathfrak{p}''} + (\mathfrak{D}_{\bar{\bar{\mathfrak{O}}}/\mathfrak{O}})_{\mathfrak{p}''},$$

$$(dx^{K'})_{\mathfrak{p}'} = (dx^K)_{\mathfrak{p}'} + (\mathfrak{D}_{\bar{\mathfrak{O}}/\mathfrak{O}})_{\mathfrak{p}'}.$$

However, ([2], p. 309, Theorem 31), $\mathfrak{D}_{\bar{\bar{\mathfrak{O}}}/\mathfrak{O}} = \mathfrak{D}_{\bar{\bar{\mathfrak{O}}}/\bar{\mathfrak{O}}} \cdot \bar{\bar{\mathfrak{O}}}\mathfrak{D}_{\bar{\mathfrak{O}}/\mathfrak{O}}$ and therefore we have:

$$\begin{aligned}(dx^{K''})_{\mathfrak{p}''} &= (dx^K)_{\mathfrak{p}''} + (\mathfrak{D}_{\bar{\bar{\mathfrak{O}}}/\bar{\mathfrak{O}}})_{\mathfrak{p}''} + e_{\mathfrak{p}''/\mathfrak{p}'} \cdot (\mathfrak{D}_{\bar{\mathfrak{O}}/\mathfrak{O}})_{\mathfrak{p}'} \\ &= e_{\mathfrak{p}''/\mathfrak{p}'}[(dx^K)_{\mathfrak{p}'} + (\mathfrak{D}_{\bar{\mathfrak{O}}/\mathfrak{O}})_{\mathfrak{p}'}] + (\mathfrak{D}_{\bar{\bar{\mathfrak{O}}}/\bar{\mathfrak{O}}})_{\mathfrak{p}''} \\ &= (dx^{K'})_{\mathfrak{p}''} + (\mathfrak{D}_{\bar{\bar{\mathfrak{O}}}/\bar{\mathfrak{O}}})_{\mathfrak{p}''}.\end{aligned}$$

We now observe that $\mathfrak{O}'$ is a quotient ring of $\bar{\mathfrak{O}}$ with respect to a multiplicative set S, and therefore we have $\bar{\bar{\mathfrak{O}}}' = \bar{\bar{\mathfrak{O}}}_s$. It follows ([2], p. 299, Theorem 27) that $(\mathfrak{D}_{\bar{\bar{\mathfrak{O}}}/\bar{\mathfrak{O}}})_{\mathfrak{p}''} = (\mathfrak{D}_{\bar{\bar{\mathfrak{O}}}'/\mathfrak{O}'})_{\mathfrak{p}''}$. On the other hand, $\mathfrak{O}''$ is a quotient ring of both $\bar{\bar{\mathfrak{O}}}$ and $\bar{\bar{\mathfrak{O}}}'$, with respect to the same multiplicative set ([2], p. 47, Theorem 18 is used implicitly here). Therefore, we have $(\mathfrak{D}_{\bar{\bar{\mathfrak{O}}}'/\mathfrak{O}'})_{\mathfrak{p}''} = (\mathfrak{D}_{\mathfrak{O}''/\mathfrak{O}'})_{\mathfrak{p}''}$, and the assertion follows.

The cases where the theorem holds for some of the other pairs of extensions are handled in an entirely similar manner and are omitted.

PROPOSITION 5. *If Theorem 2 is valid for Galois extensions K'/K, it is valid for arbitrary extensions K'/K.*

Proof. Let K'' be the least normal extension of K containing K'. Then K''/K and K''/K' are Galois. Consequently, by Proposition 4 and our assumption, Theorem 2 holds for K'/K.

We shall, therefore, assume from now on that K' is a Galois extension of K.

5. Reduction to the case in which K'/K is a cyclic extension of prime order. Let K_T, K_Z be the splitting and inertia fields, respectively, of $\mathfrak{p}'$, and let $\mathfrak{p}_Z$, $\mathfrak{p}_T$ be the contractions of $\mathfrak{p}'$ to K_Z and K_T respectively. Then it is known that $\mathfrak{p}_Z$ is unramified over $\mathfrak{p}$ ([2], p. 291, proof of Theorem 23) and that $\mathfrak{p}_T$ is unramified over $\mathfrak{p}_Z$ ([2], p. 292, Theorem 24). Hence, by the remark made at the end of Section 3, our result holds for the extensions K_Z/K and K_T/K_Z. In view of Proposition 4, we need only prove the theorem for the extension K'/K_T, i.e., we may assume from now on that $K = K_T$. The assumption $K = K_T$ leads to the (well-known) conclusion that the Galois group of K'/K is solvable. It will then follow directly, from Proposition 4, that, if the theorem is true for cyclic Galois extension of prime order, then the theorem is true for K'/K.

We shall assume from now on that K'/K is cyclic, of prime order q. Then $q = ep^s$ ($e = e_{\mathfrak{p}'/\mathfrak{p}}$), and therefore, we have either $q = e$ and $k(\mathfrak{p}') = k(\mathfrak{p})$ [3] (case of pure ramification) or $e = 1$, $q = p$, and $k(\mathfrak{p}')$ is a purely inseparable extension of $k(\mathfrak{p})$, of degree p (case of purely inseparable residue field extension). Before we present the direct arguments for these two cases, we prove a lemma relating $\mathfrak{O}'$ and $\mathfrak{O}$ (recall that $\mathfrak{O}'$ is the valuation ring of $\mathfrak{p}'$ and that $\mathfrak{O}$ is the valuation ring of $\mathfrak{p}$).

LEMMA 2. *There exists an element λ in K' such that $\mathfrak{O}' = \mathfrak{O}[\lambda]$ in either of the two cases, and, in the case of pure ramification, λ may be taken to be a uniformizing parameter of $\mathfrak{p}'$.*

Proof. Let $\lambda \in \mathfrak{O}'$ be such that $k(\mathfrak{p}') = k(\mathfrak{p})(\bar{\lambda})$ if $k(\mathfrak{p}') \neq k(\mathfrak{p})$; if $k(\mathfrak{p}') = k(\mathfrak{p})$, then let λ be a uniformizing parameter of $\mathfrak{p}'$. Let $\tilde{\mathfrak{O}} = \mathfrak{O}[\lambda]$, $\tilde{\mathfrak{M}} = \mathfrak{M}' \cap \tilde{\mathfrak{O}}$, where $\mathfrak{M}'$ is the maximal ideal in $\mathfrak{O}'$. Since $\mathfrak{p}'$ is the only extension of $\mathfrak{p}$, $\mathfrak{O}'$ is integral over $\mathfrak{O}$ and therefore also over $\tilde{\mathfrak{O}}$. Furthermore, since $\tilde{\mathfrak{M}}$ is the only prime ideal of $\tilde{\mathfrak{O}}$, $\tilde{\mathfrak{O}}$ is a local domain. We observe that $\tilde{\mathfrak{O}}/\tilde{\mathfrak{M}} = \mathfrak{O}'/\mathfrak{M}' = k(\mathfrak{p})(\bar{\lambda})$ and also that $\tilde{\mathfrak{O}}$ contains a uniformizing parameter τ of $\mathfrak{p}'$, where $\tau = \lambda$ or $\tau =$ uniformizing parameter of $\mathfrak{p}$, depending on whether or not $q = e$. Since $\lambda \notin K$, K' is the quotient field of $\tilde{\mathfrak{O}}$. We assert that $\mathfrak{O}' = \tilde{\mathfrak{O}}$. Let $\xi \in \mathfrak{O}'$. Then $\xi = \xi_0 + \eta\tau$, where $\xi_0 \in \tilde{\mathfrak{O}}$, τ is our uniformizing parameter of $\mathfrak{p}'$ in $\bar{\mathfrak{O}}$, and $\eta \in \mathfrak{O}'$, since $\bar{\mathfrak{O}}/\bar{\mathfrak{M}} = \mathfrak{O}'/\mathfrak{M}'$. It follows that, for $j \geqq 0$, there exists a $\xi_j \in \bar{\mathfrak{O}}$ such that $\xi - \xi_j \in \mathfrak{M}'^{j+1}$. Now K' is the quotient field of $\bar{\mathfrak{O}}$ and so, $\xi = a/b$ with a, b in $\bar{\mathfrak{O}}$. We then have $a - b\xi_j \in \mathfrak{M}'^{j+1} \cap \bar{\mathfrak{O}}$, i.e., $a \in \mathfrak{O}b + \mathfrak{M}'^{j+1} \cap \bar{\mathfrak{O}}$ for all $j \geqq 0$. It follows that $a \in \bar{\mathfrak{O}}b$ and hence that $\xi \in \bar{\mathfrak{O}}$. This completes the proof of the lemma.

---

[3] Since $K = K_T$.

We let $F(X) \in K[X]$ be the minimal polynomial of λ over K. Then, ([2], p. 303, Theorem 29), $\mathfrak{D}_{\mathfrak{O}'/\mathfrak{O}} = \mathfrak{O}'F'(\lambda)$, and therefore, we must show that we have $(dx^{K'})_{\mathfrak{p}'} = (dx^{K})_{\mathfrak{p}'} + (F'(\lambda))_{\mathfrak{p}'}$ in both of our two cases (where λ is chosen as in Lemma 2).

6. Direct argument in the case of pure ramification. We assume now that $q = e$ and $k(\mathfrak{p}') = k(\mathfrak{p})$. Let $\xi_1, \cdots, \xi_{\rho+1}$ be uniformizing coordinates at $\mathfrak{p}$, where ξ_1 is a uniformizing parameter of $\mathfrak{p}$ (compare with the corollary to Theorem 1). Then, it follows from Theorem 1 that $\lambda, \xi_2, \cdots, \xi_{\rho+1}$ are uniformizing coordinates at $\mathfrak{p}'$. We set $\eta_1 = \lambda$, $\eta_j = \xi_j$ for $j = 2, \cdots, \rho + 1$, and if D_i $(i = 1, \cdots, \rho + 1)$ are derivations of K such that $D_i\xi_\mu = \delta_{i\mu}$ $(i, \mu = 1, \cdots, \rho + 1)$, then we denote their extensions to K' by $\bar{D}_i$. We let $E_1, \cdots, E_{\rho+1}$ be the derivations of K' such that $E_i\eta_j = \delta_{ij}$. We have $\bar{D}_i\eta_1 = -F^{D_i}(\lambda)/F'(\lambda)$, $i = 1, \cdots, \rho + 1$, where $F^{D_i}(\lambda)$ is obtained from $F(\lambda)$ by applying D_i to the coefficients of $F(\lambda)$. Hence we have $\bar{D}_i = \sum_{\nu=1}^{\rho+1} a_{i\nu}E_\nu$, where the matrix $A = \| a_{i\nu} \|$ has the form:

$$\left[\begin{array}{c|c} -F^{D_1}(\lambda)/F'(\lambda) & 0 \cdots\cdots 0 \\ \hline -F^{D_2}(\lambda)/F'(\lambda) & \\ \vdots & I_\rho \\ -F^{D_{\rho+1}}(\lambda)/F'(\lambda) & \end{array}\right].$$

Here I_ρ is the ρ by ρ identity matrix. It follows that, if $dx du_1 \cdots du_\rho = B d\xi_1 \cdots d\xi_{\rho+1}$, then

$$dx du_1 \cdots du_\rho = B \cdot | A | \, d\eta_1 \cdots d\eta_{\rho+1} = -B(F^{D_1}(\lambda)/F'(\lambda)) d\eta_1 \cdots d\eta_{\rho+1}.$$

Therefore it will suffice to show that $F^{D_1}(\lambda)$ is a unit in $\mathfrak{O}'$.

Let $F(\lambda) = \lambda^q + a_1\lambda^{q-1} + \cdots + a_q = 0$, with $a_i \in \mathfrak{O}$. Then we have $-a_q = \lambda^q + a_1\lambda^{q-1} + \cdots + a_{q-1}\lambda$, which implies that

$$\begin{aligned} qv_{\mathfrak{p}}(a_q) &= v_{\mathfrak{p}'}(\lambda^{q-1} + \cdots + a_{q-1}) + 1 \\ &= 1 + \min\{q-1, q-2+qv_{\mathfrak{p}}(a_1), \cdots, qv_{\mathfrak{p}}(a_{q-1})\}. \end{aligned}$$

Let $a_0 = 1$ and let a_{j_0} be the coefficient such that $a_{j_0} \notin \mathfrak{M}$ and $a_j \in \mathfrak{M}$ if $j > j_0$ (here necessarily $0 \leqq j_0 < q$). Then $qv_{\mathfrak{p}}(a_q) = q - j_0$. But $v_{\mathfrak{p}}(a_q) > 0$, and therefore $j_0 = 0$ and $v_{\mathfrak{p}}(a_q) = 1$. Then $a_q = \epsilon\xi_1$, where ϵ is a unit in $\mathfrak{O}$, and we have $D_1 a_q = \xi_1 D_1\epsilon + \epsilon$, which implies that $D_1 a_q \notin \mathfrak{M}$. Since $F^{D_1}(\lambda) = (D_1 a_1)\lambda^{q-1} + \cdots + (D_1 a_q)$ and $D_1 a_i \in \mathfrak{O}$, while $v_{\mathfrak{p}'}(\lambda) = 1$, it follows that $v_{\mathfrak{p}'}(F^{D_1}(\lambda)) = 0$, and the proof for this case is now complete.

7. Direct argument in the case of purely inseparable residue field extension. We assume now that $q = p$ and that $k(\mathfrak{p}')$ is a purely inseparable extension of $k(\mathfrak{p})$. We let $\xi_1, \cdots, \xi_{\rho+1}$ be uniformizing coordinates of $\mathfrak{p}$, where we may assume (see Corollary to Theorem 1) that ξ_2 is a uniformizing parameter at $\mathfrak{p}$ (and hence also at $\mathfrak{p}'$). Now, $k(\mathfrak{p}')$ is (by our choice of λ) a separable algebraic extension of $k_1(\bar{\xi}_1, \bar{\xi}_3, \cdots, \bar{\xi}_{\rho+1}, \bar{\lambda})$ (where k_1 is our field of p-constants). We may assume that $u_1, \cdots, u_\rho$ and k_1 are p-parameters and associated field of p-constants not only for K/k and K'/k but also for $\mathfrak{p}'/k$. Under this assumption, we have, by Lemma 1, that $\dim \mathfrak{D}(k(\mathfrak{p}')/k_1) \leqq \rho$, and since $\bar{\lambda} \notin k(\mathfrak{p})$, we may assume, by the second part of Lemma 1, that $\bar{\xi}_1$ is separable algebraic over $k_1(\bar{\xi}_3, \cdots, \bar{\xi}_{\rho+1}, \bar{\lambda})$. It follows from Theorem 1 that if we let $\eta_1 = \lambda$, $\eta_j = \xi_j$, $j = 2, \cdots, \rho + 1$, then the η_i are uniformizing coordinates of $\mathfrak{p}'$. As in Section 6, we let $\{D_i\}$ be the derivations of K/k_1 such that $D_i\xi_i = \delta_{ij}$; we let $\tilde{D}_i$ denote the extension of D_i to K'; and we let $E_1, \cdots, E_{\rho+1}$ be the derivations of K' for which $E_i\eta_j = \delta_{ij}$. Arguing as in the previous section, we see that it will suffice to show that $F^{D_1}(\lambda)$ is a unit in $\mathfrak{O}'$.

Let $F(\lambda) = \lambda^p + a_1\lambda^{p-1} + \cdots + a_p = 0$, with $a_i \in \mathfrak{O}$. Since $k(\mathfrak{p})(\bar{\lambda})$ is purely inseparable over $k(\mathfrak{p})$, the coefficients $a_1, \cdots, a_{p-1}$ are in $\mathfrak{M}$. We observe that $D_1\mathfrak{M} \subset \mathfrak{M}$ and therefore that the trace of D_1 on $k(\mathfrak{p})$ (which we denote by $\bar{D}_1$) is defined.[4] If $D_1 a_p \in \mathfrak{M}$, then $\bar{D}_1$ can be extended to $k(\mathfrak{p})(\bar{\lambda})$, and we denote the extension by $\bar{D}'_1$. However, $\bar{D}'_1\bar{\eta}_j = 0$ for $j = 1, \cdots, \rho + 1$ and $\bar{D}_1\bar{\xi}_1 = 1$ together contradict the fact that $\bar{\xi}_1$ is separable algebraic over $k_1(\bar{\eta}_1, \cdots, \bar{\eta}_{\rho+1})$. It follows that $D_1 a_p \notin \mathfrak{M}$. Since we have $F^{D_1}(\lambda) = (D_1 a_1)\lambda^{p-1} + \cdots + (D_1 a_p)$ and $D_1 a_i \in \mathfrak{M}$ if $i < p$, it follows at once that $v_{\mathfrak{p}'}(F^{D_1}(\lambda)) = 0$ and the proof is now complete also in this case.

HARVARD UNIVERSITY.

REFERENCES.

[1] O. Zariski, "The concept of a simple point of an abstract algebraic variety," *Transactions of the American Mathematical Society*, vol. 62, 1-52 (1947).

[2] O. Zariski and P. Samuel, "Commutative Algebra," vol. I, Princeton, D. Van Nostrand Co., 1958.

---

[4] It is given by: $\bar{D}_1\bar{z} = \overline{D_1 z}$, $z \in \mathfrak{O}$.

POLYHEDRA IN S^n WHOSE COMPLEMENTS HAVE UNIFORMLY ABELIAN LOCAL FUNDAMENTAL GROUPS.*[1]

By C. H. Edwards, Jr.

---

1. Introduction.

If E and F are homeomorphic closed subsets of the n-sphere S^n, then a necessary condition that an arbitrary homeomorphism carrying E onto F will admit an extension to S^n is that the fundamental groups $\pi_1(S^n - E)$ and $\pi_1(S^n - F)$ of their complementary domains be isomorphic. O. G. Harrold [4] has investigated the problem of imposing local conditions on the complements of certain homeomorphic closed sets in S^n which will suffice to imply that the corresponding fundamental groups vanish. He shows in particular that if C is an i-cell in S^n with $S^n - C$ having uniformly abelian local fundamental groups, then $\pi_1(S^n - C) = 1$. A generalization of the proof of Harrold is here employed to extend this result to a certain class of contractible $(n-1)$-dimensional curvilinear polyhedra imbedded in S^n.

2. Notation and definitions.

The notation and definitions used here are the same as those used by Harrold in [4]. In particular, the open set A in the space X will be said to have *uniformly abelian local fundamental groups* provided that for each point $p \in X$ and each neighborhood U of p in A, there is a neighborhood V of p such that $V \subset U$ and such that every closed path in V which is homotopic (in U) to the commutator of two paths in U is nullhomotopic in U.

3.

Theorem 1. *Suppose that C is a curved polyhedral complex imbedded in S^n, $n \leqq 5$, such that*

(a) $C = \bigcup_{i=1}^{k} D_i$, $i = 1, \cdots, k$, *being $(n-1)$-cell subcomplexes of C such that* $\operatorname{Int} D_j \cap \bigcup_{i \neq j} D_i = \square$, $j = 1, \cdots, k$.

(b) $D_j \cap \bigcup_{i=1}^{j-1} D_i$, $j = 2, \cdots, k$, *is an $(n-2)$-cell complex tamely imbedded in the $(n-2)$-sphere* $\operatorname{Bd} D_j$.

---

* New version received January 17, 1961.

[1] This paper was supported in part by the National Science Foundation, Contract G-8239.

If $S^n - C$ *has uniformly abelian local fundamental groups, then* $\pi_1(S^n - C) = 1$.

The dimensional restriction $n \leqq 5$ arises from the use of the following conjecture, which has been proved in the case $n \leqq 5$ by Guggenheim [3]:

Conjecture A. *If* P^{n-2} *is a polyhedral* $(n-2)$*-cell in* S^{n-1}, *then* P^{n-2} *is flat in* S^{n-1} (there exists a piecewise-linear isotopy of S^{n-1} carrying P^{n-2} onto a standard $(n-2)$-simplex).

If Conjecture A holds for all dimensions, then Theorem 1 holds for all dimensions. Observe that the tameness hypothesis in (b) is unnecessary for $n \leqq 5$.

4. Outline of proof. Generalizing the construction employed by Harrold in [4], a separable metric subspace $X = A \cup M$ of the Hilbert cube is defined, with A being ULC^1 and homeomorphic to $S^n - C$, and with M being a topological $(n-1)$-sphere constituting the boundary in X of A. M is then clearly LC^1 with $\pi_1(M) = 1$. It is shown also that $\pi_1(A, X) = 1$, so that a theorem of Eilenberg and Wilder [2, Theorem 8] applies directly to show that $\pi_1(A) = 1$, which implies that $\pi_1(S^n - C) = 1$, A and $S^n - C$ being homeomorphic.

5.

5.1. *Preliminaries.* By the order of a point $a \in C$ will be meant the positive integer $p^{n-1}(a, C) + 1$, where $p^{n-1}(a, C)$ is the $(n-1)$-dimensional Betti number of C around the point a [1, § 1]. Denote by $C^{(k)}$ the subset of all points of C of order k. It is clear that $C^{(2)} = \bigcup_{i=1}^{k} \operatorname{Int} D_i$ is an open (in C) dense subset of C.

Hence given any point $a \in \operatorname{Int} D_j$, $1 \leqq j \leqq k$, $\delta_a \geqq 0$ can be chosen sufficiently small that $S(a, \delta_a) - C = S(a, \delta_a) - D_j = U_a \cup V_a$, with U_a and V_a separated by D_j [1, § 2]. It may be assumed that the notation is chosen in such a manner that

$$U_j = \bigcup_{a \in \operatorname{Int} D_j} U_a \text{ and } V_j = \bigcup_{a \in \operatorname{Int} D_j} V_a$$

are disjoint open connected sets separated in $U_j \cup V_j \cup D_j$ by D_j. (This can be done as in [5, p. 280]). It will be said that a point $x \in S^n - C$ sufficiently near D_j lies on the positive or negative side of D_j according as $x \in U_j$ or $x \in V_j$ respectively.

Now let $\{p^j_m\}_{m=1}^{\infty}$ be a countable dense subset of $\operatorname{Int} D_j$. For each m

choose $\delta_m > \epsilon_m > 0$ such that $S(p^j{}_m, \delta_m) - C = U^m \cup V^m$ with $U^m \subset U_j$ and $V^m \subset V_j$ and such that any connected subset of $S^n - C$ joining a point in $U^m \cap S(p^j{}_m, \epsilon_m)$ with a point in $V^m \cap S(p^j{}_m, \epsilon_m)$ must have a diameter $> 2\epsilon_m$. For each m choose an arc $l_m = p^j{}_m q^j{}_m$, with $l_m - p^j{}_m \subset S(p^j{}_m, \epsilon_m) - C$, in such a way that each of the two subsequences

$$\{p^j{}_m \mid q^j{}_m \in U_j\} \text{ and } \{p^j{}_m \mid q^j{}_m \in V_j\}$$

is dense in D_j.

The countable dense subset $\bigcup_{j=1}^{k} \{p^j{}_m\}_{m=1}^{\infty}$ of C is then ordered in such a manner as to obtain a sequence $\{p_i\}_{i=1}^{\infty}$ such that $p_i \in \operatorname{Int} D_j$ if and only if $i \equiv j \pmod{k}$. That is, the subsequence of $\{p_i\}_{i=1}^{\infty}$ which is contained in $\operatorname{Int} D_j$ is precisely the subsequence $\{p_{j+mk}\}_{m=0}^{\infty}$.

5.2. *Definition of* A. Proceeding in this section as in 4.6 of [4], define a sequence $\{f_i\}_{i=1}^{\infty}$ of real-valued continuous functions on $S^n - C$ by $f_i(x) = \rho(x, q_i)$ for $x \in S^n - C$, where the "relative distance metric" ρ is defined on $S^n - C$ by $\rho(x, y) =$ g. l. b. of the diameters of all connected subsets of $S^n - C$ containing both x and y.

A homeomorphism h carrying $S^n - C$ into Hilbert space is defined as follows: If $(x_1, \cdots, x_n) = x \in S^n - C$, let $h(x) = \{x_1, \cdots, x_n, f_1(x), f_2(x), \cdots\}$. Denote by A the image set $h(S^n - C)$. Assume that a metric μ is defined in A as in 4.64 of [4].

5.3. Since $S^n - C$ by hypothesis has uniformly abelian local fundamental groups, the techniques used in 4.7 and 4.71 of [4] apply with slight modification to show that A is ULC^1.

5.4. *Definition of* M. Let $C_j = \bigcup_{i=1}^{j} D_i$ for each $j = 1, \cdots, k$ so that $C_1 = D_1$ and $C_k = C$. For each $j = 1, \cdots, k$ let the metric ρ_j be defined on $S^n - C_j$ by $\rho_j(x, y) =$ g. l. b. of the diameters of all connected subsets of $S^n - C_j$ containing both x and y, and define k sequences of real-valued functions $\{f_{ij}\}_{i=1}^{\infty}$, $j = 1, \cdots, k$, by $f_{ij}(x) = \rho_j(x, q_i)$.

Suppose now that D_s is an $(n-1)$-cell in C_j and let U_s and V_s be the corresponding open sets defined in 5.1, such that $U_s \cup V_s \cup \operatorname{Int} D_s$ is a neighborhood of $\operatorname{Int} D_s$ with U_s and V_s separated in $U_s \cup V_s \cup D_s$ by D_s. If $x \in \operatorname{Int} D_s$ and $i \equiv 1, 2, \cdots, j \pmod{k}$ then define $f_{ij}'(x) = \lim_{\bar{x} \to x} f_{ij}(x)$ for $\bar{x} \in U_s$ and $f_{ij}''(x) = \lim_{\bar{x} \to x} f_{ij}(x)$ for $x \in V_s$. If $i \equiv j + 1, \cdots, k \pmod{k}$, then define $f_{ij}'(x) = f_{ij}''(x) = 0$. Since two points close to x both lying either in U_s or V_s can be joined by a connected set of small diameter, it is clear that the functions f_{ij}' and f_{ij}'' are thereby uniquely defined.

If $x \in \operatorname{Int} D_s$, define

$$h_j'(x) = \{x_1, \cdots, x_n, f_{1j}'(x), f_{2j}'(x), \cdots\},$$
$$h_j''(x) = \{x_1, \cdots, x_n, f_{1j}''(x), f_{2j}''(x), \cdots\}.$$

If $y \in \operatorname{Bd} D_s$, define $h_j'(x) = \lim\limits_{x \to y} h_j'(x)$ and $h_j''(y) = \lim\limits_{x \to y} h_j''(x)$ for $x \in \operatorname{Int} D_s$. Then h_j' and h_j'', $j = 1, \cdots, k$, are mappings of D_s into a Hilbert cube (with the metric referred to in 5.2). If $x \in D_s \cap C^{(1)}$, then C_j does not separate sufficiently small neighborhoods of x, and it follows that $h_j'(x) = h_j''(x)$. But if $x \in D_s \cap C^{(k)}$, $k > 1$, then C_j does separate sufficiently small neighborhoods of x, and it follows that $h_j'(x) \neq h_j''(x)$.

5.41. An elementary continuity argument similar to that used in 4.8 of [4] suffices to show that h_j' and h_j'' are homeomorphisms on D_s, so that $h_j'(D_s)$ and $h_j''(D_s)$ are $(n-1)$-cells, $j = 1, \cdots, k$; $s = 1, \cdots, j$. The manner in which these homeomorphisms match on the boundaries of two intersecting cells D_r and D_s is described in the following section.

5.42. Suppose that z is a point of $C^{(k)}$ common to the boundaries of the $(n-1)$-cells D_r and D_s in C_j. If $\delta > 0$ is sufficiently small, then $S(z, \delta) - C_j$ consists of k mutually separated open sets. Suppose that W is one of these sets intersecting both U_r and U_s. Then it follows that $\lim h_j'(x)$ with $x \to z$, $x \in D_r$, is equal to $\lim h_j'(y)$ with $y \to z$, $y \in D_s$. To see this, notice that if $x \in \operatorname{Int} D_r$ and $y \in \operatorname{Int} D_s$ are sufficiently near z, and if $\bar{x} \in U_r$ and $\bar{y} \in U_s$ are sufficiently near x and y respectively, then $\bar{x}$ and $\bar{y}$ are both in W and can be joined in $S^n - C_j$ by a connected set of small diameter. Taking limits as $\bar{x} \to x$, $\bar{y} \to y$, and $x \to z \leftarrow y$ gives the desired result.

5.43. Now define $M_j = \bigcup\limits_{i=1}^{j} [h_j'(D_i) \cup h_j''(D_i)]$, $j = 1, \cdots, k$. Clearly $M = M_k$ is the boundary in $X = A \cup M$ of A.

5.5. *Proof that M is an $(n-1)$-sphere.* It will now be shown that $M = M_k$ is an $(n-1)$-sphere. That M_1 is an $(n-1)$-sphere follows as in 4.8 of [4]. The induction proof will be completed by showing that the assumption that M_j is an $(n-1)$-sphere implies that M_{j+1} is an $(n-1)$-sphere, $j = 1, \cdots, k-1$.

For each $x \in L_{j+1} = C_j \cap D_{j+1}$, define $f_{ij}^*(x) = \lim f_{ij}(\bar{x})$ for $\bar{x} \to x$, $\bar{x} \in D_{j+1}$

if $i \equiv 1, \cdots, j \pmod{k}$ and $f_{ij}^*(x) = 0$ if $i \equiv j+1, \cdots, k \pmod{k}$. Then define

$$h_j^*(x) = \{x_1, \cdots, x_n, f_{1j}^*(x), f_{2j}^*(x), \cdots\}.$$

It follows from 5.41 that $h_j^*(L_{j+1})$ is homeomorphic with L_{j+1} and is hence an $(n-2)$-cell.

Now triangulate M_j in the following natural manner: Recalling that each D_i is a subcomplex of M_j, choose for $h_j'(D_j)$ and $h_j''(D_i)$ the subdivisions induced by the homeomorphisms h_j' and h_j'' and the original subdivision of D_i. Since $M_j = \bigcup_{i=1}^{j} [h_j'(D_i) \cup h_j''(D_i)]$, this suffices to triangulate M_j.

Since L_{j+1} is by hypothesis a subcomplex of C, it follows immediately that $h_j^*(L_{j+1})$ is a subcomplex of M_j, that is, that the $(n-2)$-cell $h_j^*(L_{j+1})$ is polyhedrally imbedded in the $(n-1)$-sphere M_j.

5.51. Now define a mapping ϕ of $\bigcup_{i=1}^{j} [h_{j+1}'(D_i) \cup h_{j+1}''(D_i)]$ onto M_j by setting $\phi(x) = h_j' h_{j+1}'^{-1}(x)$ for $x \in h_{j+1}'(D_i)$ and $\phi(x) = h_j'' h_{j+1}''^{-1}(x)$ for $x \in h_{j+1}''(D_i)$. Observe that ϕ is clearly 1-1 bicontinuous except at points of $h_{j+1}'(L_{j+1}) \cup h_{j+1}''(L_{j+1})$. Indeed ϕ carries each of the $(n-2)$-cells $h_{j+1}'(L_{j+1})$ and $h_{j+1}''(L_{j+1})$ homeomorphically onto the $(n-2)$-cell $h_{j+1}^*(L_{j+1})$, and carries the $(n-1)$-cells $h_{j+1}'(D_i)$ and $h_{j+1}''(D_i)$ homeomorphically onto the $(n-1)$-cells $h_j'(D_i)$ and $h_j''(D_i)$ respectively, $i = 1, \cdots, j$. It follows as in 5.42 that ϕ is single-valued.

Since $h_j^*(L_{j+1})$ is a polyhedral $(n-2)$-cell in the $(n-1)$-sphere M_j, there exists, by Conjecture A, a homeomorphism f of M_j onto itself carrying $h_j^*(L_{j+1})$ onto a standard $(n-2)$-simplex P.

Now let E be an $(n-1)$-simplex with base P and opposite vertex p. Let q be an interior point of P and let p' be an interior point of the interval qp. Then denote by E' the $(n-1)$-simplex with base P and opposite vertex p'. Let g be the mapping defined as follows:

a) $g(x) = x$ if $x \in \mathrm{Cl}(M_j - E)$;

b) If $x \in P$, denote by x' the point of intersection of the segment xp with $\mathrm{Bd}\, E' - P$. Then let g contract the segment xp linearly onto the segment $x'p$. Clearly g gives a homeomorphism of $M_j - P$ onto $M_j - E'$, but each point $a \in \mathrm{Int}\, P$ has two image points: $g'(a) = a \in P$ and $g''(a) \in \mathrm{Bd}\, E' - P$.

A homeomorphism ψ of $\bigcup_{i=1}^{j} [h_{j+1}'(D_i) \cup h_{j+1}''(D_i)]$ onto the closed $(n-1)$-cell $\mathrm{Cl}(M_j - E')$ is now defined. If $x \notin h_{j+1}'(L_{j+1}) \cup h_{j+1}''(L_{j+1})$, let $\psi(x) = gf\phi(x)$. If $x \in h_{j+1}'(L_{j+1})$ define $\psi(x) = g'f\phi(x)$ and if $x \in h_{j+1}''(L_{j+1})$

define $\psi(x) = g''f\phi(x)$. It is immediate that ψ is a homeomorphism, so that $\bigcup_{i=1}^{j} [h_{j+1}'(D_i) \cup h_{j+1}''(D_i)]$ is a closed $(n-1)$-cell.

5.52. It is shown that $h_{j+1}'(D_{j+1}) \cup h_{j+1}''(D_{j+1})$ is a closed $(n-1)$-cell. By 5.41, $h_{j+1}'(D_{j+1})$ and $h_{j+1}''(D_{j+1})$ are both closed $(n-1)$-cells. If $x \in \operatorname{Int} L_{j+1} \cup \operatorname{Int} D_{j+1}$, then $h_{j+1}'(x)$ and $h_{j+1}''(x)$ are distinct, while $h_{j+1}'(x) = h_{j+1}''(x)$ if $x \in \operatorname{Bd} D_{j+1} - \operatorname{Int} L_{j+1}$. Thus $h_{j+1}'(D_{j+1})$ and $h_{j+1}''(D_{j+1})$ are two $(n-1)$-cells meeting in $h_{j+1}(\operatorname{Bd} D_{j+1} - \operatorname{Int} L_{j+1})$. Since by hypothesis L_{j+1} is tamely imbedded in the $(n-2)$-sphere $\operatorname{Bd} D_{j+1}$, it follows that $\operatorname{Bd} D_{j+1} - \operatorname{Int} L_{j+1}$ is a closed $(n-2)$-cell tamely imbedded in $\operatorname{Bd} D_{j+1}$. Hence $h_{j+1}(\operatorname{Bd} D_{j+1} - \operatorname{Int} L_{j+1})$ is a closed $(n-2)$-cell tame in each of the boundaries of the two $(n-1)$-cells $h_{j+1}'(D_{j+1})$ and $h_{j+1}''(D_{j+1})$. It follows easily that $h_{j+1}'(D_{j+1}) \cup h_{j+1}''(D_{j+1})$ is a closed $(n-1)$-cell.

Consequently $M_{j+1} = \bigcup_{i=1}^{j+1} [h_{j+1}'(D_i) \cup h_{j+1}''(D_i)]$ is the union of the two closed $(n-1)$-cells $\bigcup_{i=1}^{j} [h_{j+1}'(D_i) \cup h_{j+1}''(D_i)]$ and $h_{j+1}'(D_{j+1}) \cup h_{j+1}''(D_{j+1})$ intersecting in their common boundary, the $(n-2)$-sphere $h_{j+1}'(L_{j+1}) \cup h_{j+1}''(L_{j+1})$. Hence M_{j+1} is an $(n-1)$-sphere, and it follows by induction that M is an $(n-1)$-sphere.

6. Since M is an $(n-1)$-sphere, M is LC^1 with $\pi_1(M) = 1$. Since the proof of 4.9 of [4] applies without alteration to show that $\pi_1(A, X) = 1$, Theorem 8 of [2] now implies that $\pi_1(A) = 1$. Since A was constructed homeomorphic to $S^n - C$, it follows that $\pi_1(S^n - C) = 1$. This completes the proof of Theorem 1.

UNIVERSITY OF TENNESSEE.

REFERENCES.

[1] P. Alexandroff, "Local properties of closed sets," *Annals of Mathematics*, vol. 36 (1935), pp. 1-35.

[2] S. Eilenberg and R. L. Wilder, "Uniform local connectedness and contractibility," *American Journal of Mathematics*, vol. 64 (1942), pp. 613-622.

[3] V. K. A. M. Gugenheim, "Piecewise linear isotopy and imbedding of elements and spheres, II," *Proceedings of the London Mathematical Society*, Series 3, vol. 3 (1953), pp. 129-152.

[4] O. G. Harrold, Jr., "Euclidean domains with uniformly abelian local fundamental groups," *Transactions of the American Mathematical Society*, vol. 67 (1949), pp. 120-129.

[5] ———, "Locally Peripherally unknotted surfaces in E^3," *Annals of Mathematics*, vol. 69 (1959), pp. 276-290.

EXISTENCE OF UNIVERSAL CONNECTIONS.*

By M. S. Narasimhan and S. Ramanan.

1. Introduction. The purpose of this paper is to prove the existence of universal connections for principal bundles with a compact Lie group as structure group. We prove (Theorem 2) that given a compact Lie group G and a positive integer n, there exist a differentiable principal G-bundle E *and* a connection γ_0 on E such that any connection on a differentiable principal G-bundle P with base of dimension $\leqq n$ can be obtained as the inverse image of the connection γ_0 by a differentiable bundle homomorphism of P into E. As is well-known, the analogous problem for bundles without connections is treated in the topology of fibre bundles [1].

It is also known that the Stiefel bundles play the role of universal bundles for the unitary groups $U(k)$. One can define in a natural way a connection on every Stiefel bundle (§ 2). We prove that these connections themselves are universal for connections in $U(k)$-bundles. A precise formulation is found in Theorem 1.

In the unitary case the problem is first solved locally by explicit construction, the crucial step being the lemma in § 3. The local solutions are then pieced up with the help of a special type of covering by coordinate cells.

In the general case, the compact Lie group G is identified with a closed subgroup of a unitary group. Starting from a universal connection for this unitary group, a universal connection for G is constructed by generalizing the usual method of construction of an invariant connection in the principal bundle associated with a Lie group and a closed subgroup ([3], p. 45).

A theorem of A. Weil ([1], p. 57) asserts that the cohomology classes of the base of a principal G-bundle obtained by substitution of the curvature form of a connection on P in the invariant polynomials of G are independent of the connection. Our result seems to explain this invariance and in fact furnishes an alternate proof in the case of compact Lie groups.

For definitions of the notions related to connections in principal bundles we refer to [1] and [3]. We use connections and connection forms interchangeably. By " differentiable " we always mean " indefinitely differentiable."

---

* Received February 10, 1961.

All manifolds, bundles, bundle homomorphisms and differential forms are assumed to be differentiable. Also all manifolds that occur are paracompact.

We are thankful to Professor K. Chandrasekharan for his constant encouragement and interest.

2. Canonical connections in Stiefel bundles. Let $\boldsymbol{C}^N$ be the N-dimensional complex number space with O as origin. The Stiefel manifold $V(N,k)$ (with $N \geqq k$) of all unitary k-frames at O may then be identified with the left coset space $U(N)/I_k \times U(N-k)$ where I_k is the unit (k,k) matrix. To every frame $(v_1, \cdots, v_k)$ with $v_i = \sum_{j=1}^{N} b_{i,j} e_j$ where (e_j) is the canonical base in $\boldsymbol{C}^N$, we associate the (N,k)-matrix $A = (a_{i,j})$ with $a_{i,j} = b_{j,i}$. Since $(v_1, \cdots, v_k)$ is orthonormal, we have $\sum_{\alpha=1}^{N} b_{j,\alpha} \bar{b}_{l,\alpha} = \delta_{j,l}$, i. e. A satisfies the condition $A^*A = I_k$ where A^* is the conjugate transpose of A. Thus $V(N,k)$ is identified with (N,k) matrices A satisfying $A^*A = I_k$. The action of $U(k)$ (resp. $U(N)$) on $V(N,k)$ to the right (resp. to the left) goes over under the above identification into multiplication of (N,k) matrices by unitary (k,k) matrices on the right (resp. by unitary (N,N) matrices on the left). Under the action of $U(k)$, $V(N,k)$ becomes a principal $U(k)$-bundle (known as the Stiefel bundle) with the Grassman manifold $G(N,k)$ of k-subspaces of $\boldsymbol{C}^N$ as base. $G(N,k)$ may again be identified with the left coset space $U(N)/U(k) \times U(N-k)$.

Let S be the (N,k) matrix-valued function on $V(N,k)$ which associates to each frame $(v_1, \cdots, v_k)$ the matrix A. Consider the (k,k) matrix-valued differential form S^*dS on $V(N,k)$. Since $S^*S = I_k$ for every frame, on differentiation we obtain $S^*dS + (dS^*)S = 0$, or again $S^*dS + (S^*dS)^* = 0$. Hence S^*dS has actually values in the Lie algebra $\mathfrak{u}(k)$ (which is the vector space of skew-Hermitian matrices) of $U(k)$.

PROPOSITION 1. *S^*dS is a connection form on the Stiefel bundle $V(N,k)$ which is invariant under the action of $U(N)$.*

In fact, if X_ξ is a tangent vector at $\xi \in V(N,k)$ and $s \in U(k)$, we shall denote by $X_\xi s$ the image of X_ξ under the differential of the map $\xi \to \xi s$ of $V(N,k)$. Then we have

$$\begin{aligned}(S^*dS)(X_\xi s) &= S^*(\xi s)(X_\xi s)(S)\\ &= s^*S^*(\xi)(X_\xi S)s\\ &= s^{-1}(S^*dS)(X_\xi)s.\end{aligned}$$

On the other hand, if $a \in \mathfrak{u}(k)$, we identify a with a tangent vector at e and denote by ξa the image of a under the differential of the map $s \rightarrow \xi s$ of G into $V(N,k)$. Then

$$\begin{aligned}(S^*dS)(\xi a) &= S(\xi)^*(\xi a)(S)\\ &= S(\xi)^*S(\xi)a\\ &= a,\end{aligned}$$

since $S(\xi)^*S(\xi) = I_k$. Hence S^*dS is a connection form on the Stiefel bundle. Moreover, if $t \in U(N)$, the left translation of the differential form by t yields $(tS)^*d(tS) = S^*t^*tdS = S^*dS$.

Remark. This connection will hereafter be referred to as the canonical connection and will be denoted by γ_0.

The horizontal subspace for this connection at the point $\xi_0 = \begin{pmatrix} I_k \\ 0 \end{pmatrix}$ of $V(N,k)$ may be described as follows: The tangent space at ξ_0 can be identified with (N,N) skew Hermitian matrices of the type $\begin{pmatrix} P & -Q^* \\ Q & 0 \end{pmatrix}$ where P is a (k,k) skew Hermitian matrix and Q is a rectangular $(N, N-k)$ matrix. The horizontal vectors at ξ_0 for the connection γ_0 are then given by matrices of the type $\begin{pmatrix} 0 & -Q^* \\ Q & 0 \end{pmatrix}$. This description together with the invariance under the action of $U(N)$ characterises the connection γ_0 completely.

Analogous statements are true for the real Stiefel manifold $W(N,k)$ and the corresponding $O(k)$-bundle. In particular $S'dS$ (where S' is the transpose of S) is a connection form on the Stiefel bundle, the corresponding horizontal subspace at ξ_0 being given by matrices of the type $\begin{pmatrix} 0 & -Q' \\ Q & 0 \end{pmatrix}$. This is easily seen to be the orthogonal complement of the vertical subspace at ξ_0 with respect to the killing form $\operatorname{tr}(\operatorname{ad}x \operatorname{ad}y)$ on $\mathfrak{o}(k)$, the Lie algebra of $O(k)$.

3. The local problem.

LEMMA. *Let U be an open subset of $\mathbf{R}^n$ and V a relatively compact open subset whose closure is contained in U. For every differential form α of degree 1 on U with values in $\mathfrak{u}(k)$ (the space of skew-Hermitian matrices), there exist differentiable functions $\phi_1, \cdots, \phi_{m'}$ in V with values in the space $\mathfrak{M}_k(\boldsymbol{C})$ of (k,k) complex matrices such that*

i) $$\sum_{j=1}^{m'} \phi_j^*\phi_j = I_k, \quad \textit{and}$$

ii) $$\sum_{j=1}^{m'} \phi_j^* d\phi_j = \alpha,$$

where $m' = (2n+1)k^2$.

Proof. Let $f_1, \cdots, f_{k^2}$ be a set of positive definite matrices which form a base for the complex Hermitian matrices over the reals, such that $\| f_r \| = 1$ for every r ($\| f \|$ being the norm as a linear transformation). Since α has values in $\mathfrak{u}(k)$, we may write α/i in U as $\sum_{s=1}^{n} \sum_{r=1}^{k^2} \lambda_{r,s} f_r dx_s$, where $\lambda_{r,s}$ are real-valued functions and x_s the coordinate functions in $\boldsymbol{R}^n$. If $a_{r,s} = \sup_V | \lambda_{r,s} |$, we have $\lambda_{r,s} = \mu_{r,s} - \nu_{r,s}$ where

$$\mu_{r,s} = \tfrac{1}{2}\{\lambda_{r,s} + a_{r,s} + 1\} \quad \text{and}$$

$$\nu_{r,s} = \tfrac{1}{2}\{a_{r,s} - \lambda_{r,s} + 1\}$$

are both strictly positive differentiable functions. Hence we may write $\mu_{r,s} = p_{r,s}{}^2$ and $\nu_{r,s} = q_{r,s}{}^2$ where $p_{r,s}$ and $q_{r,s}$ are positive differentiable functions. Clearly one may assume that $\sum_{s=1}^{n} (\mu_{r,s} + \nu_{r,s})$ is bounded by $1/2k^2$ on V for every r, by altering the coordinate functions x_s by a constant multiple, if necessary. The matrix valued function $1/k^2 I_k - \{\sum_{s=1}^{n} (\mu_{r,s} + \nu_{r,s})\} f_r$ is then positive. For,

$$\| \sum_{s=1}^{n} (\mu_{r,s} + \nu_{r,s}) f_r \| \leqq 1/2k^2 \| f_r \| < 1/k^2.$$

Let g_r be the (unique) positive square-root of the positive matrix f_r and h_r the differentiable positive matrix-valued function satisfying

$$h_r{}^2(x) = 1/k^2 I_k - \{ \sum_{s=1}^{n} (\mu_{r,s}(x) + \nu_{r,s}(x)) \} f_r.$$

We now define $\mathfrak{M}_k(\boldsymbol{C})$-valued functions $\phi_j (1 \leqq j \leqq (2n+1)k^2)$ as follows.

For $1 \leqq j \leqq nk^2$, ϕ_j shall be the nk^2 functions $p_{r,s} e^{ix_s} \cdot g_r$ arranged in some order.

For $nk^2 + 1 \leqq j \leqq 2nk^2$, ϕ_j shall be the nk^2 functions $q_{r,s} e^{-ix_s} \cdot g_r$ arranged in some order.

For $2nk^2 + 1 \leqq j \leqq (2n+1)k^2$, ϕ_j shall be the functions h_r in some order.

We have to verify that the ϕ_j thus defined fulfil the conditions i) and ii) of the lemma. In fact,

$$\begin{aligned}\sum_{j=1}^{m'}\phi_j{}^*\phi_j &= \sum_{r,s} p_{r,s}{}^2 g_r{}^2 + \sum_{r,s} q_{r,s}{}^2 g_r{}^2 + \sum_r h_r{}^2 \\ &= \sum_{r,s}\mu_{r,s}f_r + \sum_{r,s}\nu_{r,s}f_r + I_k - \sum_{r,s}(\mu_{r,s}+\nu_{r,s})f_r \\ &= I_k.\end{aligned}$$

On the other hand,

$$\begin{aligned}\sum_{j=1}^{m'}\phi_j{}^*d\phi_j &= \sum_{r,s} p_{r,s}e^{-ix_s}\{p_{r,s}ie^{ix_s}(dx_s) + (dp_{r,s})e^{ix_s}\}g_r{}^2 \\ &\quad + \sum_{r,s} q_{r,s}e^{ix_s}\{-q_{r,s}\cdot ie^{-ix_s}(dx_s) + (dq_{r,s})e^{-ix_s}\}g_r{}^2 \\ &\quad + \sum_r h_r dhr \\ &= \sum_{r,s} i\cdot p_{r,s}{}^2 g_r{}^2 dx_s + \sum_{r,s} p_{r,s}dp_{r,s}g_r{}^2 \\ &\quad + \sum_{r,s} i(-q_{r,s}{}^2)g_r{}^2 dx_s + \sum_{r,s} q_{r,s}dq_{r,s}g_r{}^2 + \sum_r h_r dh_r \\ &= \sum_{r,s} i(\mu_{r,s}-\nu_{r,s})f_r dx_s + \tfrac{1}{2}\sum_{r,s} d(p_{r,s}{}^2 + q_{r,s})f_r + \sum_r h_r dh_r \\ &= \alpha + \tfrac{1}{2}\sum_{r,s} d(\mu_{r,s}+\nu_{r,s})f_r + \sum_r h_r dh_r.\end{aligned}$$

But since for any $x, y \in V$, $h_r{}^2(x)$ and $h_r{}^2(y)$ commute, their positive square roots $h_r(x)$ and $h_r(y)$ also commute. It readily follows that $h_r dh_r = dh_r\cdot h_r$. Hence $\frac{1}{2}d(h_r{}^2) = h_r dh_r$. Therefore, finally we have

$$\begin{aligned}\sum_{j=1}^{m'}\phi_j{}^*d\phi_j &= \alpha + \tfrac{1}{2}d\{\sum_{r,s}(\mu_{r,s}+\nu_{r,s})f_r + \sum_r h_r{}^2)\} \\ &= \alpha,\end{aligned}$$

since $\sum_{r,s}(\mu_{r,s}+\nu_{r,s})f_r + \sum_r h_r{}^2 = I_k$, and the lemma is completely proved.

The problem is solved locally by the following

PROPOSITION 2. Let P be a principal $U(k)$-bundle over a manifold X of dimension $\leqq n$ and γ a connection form on P. For every relatively compact open subset W of X with $\bar{W}$ contained in a coordinate neighborhood U of X over which P is trivial, there exists a differentiable bundle map Φ of $p^{-1}(W)$ into $V(m'', k)$ such that the inverse image of the canonical connection γ_0 by Φ is γ, where $m'' = (2n+1)k^3$ and p is the projection $P \to X$.

Proof. Let σ be a section of P over U and α the inverse image of γ by σ.

By the lemma, we can find differentiable $\mathfrak{M}_k(C)$-valued functions $\phi_1, \cdots, \phi_{m'}$ in W such that

i) $\sum_{j=1}^{m'} \phi_j^* \phi_j = I_k$, and

ii) $\sum_{j=1}^{m'} \phi_j^* d\phi_j = \alpha$, where $m' = (2n+1)k^2$.

Define a map Φ of P over W into the space of (m'', k)-matrices by setting for $\xi \in P$, $\Phi(\xi) = \begin{pmatrix} \phi_1(p\xi) \\ \vdots \\ \phi_{m'}(p\xi) \end{pmatrix} \cdot s$ where $s \in U(k)$ is determined by $\xi = \sigma(p\xi)s$.

Φ is easily seen to be a bundle homomorphism. We then have

$$\begin{aligned} \Phi^*\Phi(\xi) &= s^*\left(\sum_{j=1}^{m'} (\phi_i^*\phi_i)(p\xi)\right)s \\ &= s^*s, \text{ by (i)} \\ &= I_k, \text{ since } s \text{ is unitary.} \end{aligned}$$

Hence Φ maps $P|p^{-1}(W)$ actually into $V(m'', k)$. On the other hand, it is obvious that the inverse image by Φ of $\gamma_0 = S^* dS$ is given by $\Phi^* d\Phi$. But the inverse image by σ of $\Phi^* d\Phi$ is $(\Phi \circ \sigma)^* d(\Phi \circ \sigma) = \sum_{i=1}^{m'} \phi_i^* d\phi_i = \alpha$ by construction. Now γ and $\Phi^* d\Phi$ are two connections on $P|p^{-1}(W)$ such that their inverse image by the section σ are the same. Hence $\gamma = \Phi^* d\Phi$ on $p^{-1}(W)$.

4. Universal connection for the unitary group.

THEOREM 1. *Let P be a principal $U(k)$-bundle over a manifold X of dimension $\leq n$ and γ any connection form on P. Then there exists a differentiable bundle homomorphism Φ of P into the Stiefel bundle $V(m, k)$ such that γ is the inverse image by Φ of the canonical connection γ_0 on $V(m, k)$, where $m = (n+1)(2n+1)k^3$.*

Proof. We can find a covering of X by relatively compact open sets $\{V_i\}$ such that i) each $\bar{V}_i$ is contained in a coordinate cell, and ii) the V_i's can be divided into $(n+1)$ classes $\mathcal{B}_j$ in such a way that no two V_i's of the same class intersect ([2], p. 61). Let $\{W_i\}$ be a shrinking of this covering, i. e., an open covering $\{W_i\}$ such that $\bar{W}_i \subset V_i$. Let D_j $(j = 1, \cdots, n+1)$ be the union of the open sets $p^{-1}(W_i)$ where $\bar{W}_i \subset V_i$ with V_i belonging to $\mathcal{B}_j$.

The bundle is trivial over the coordinate cells and hence, by Proposition 2, one can find differentiable bundle homomorphisms Φ_i on $p^{-1}(V_i)$ into

$V((2n+1)k^3, k)$ inducing the connection γ on $p^{-1}(V_i)$. Corresponding to each D_j there exists a $\{(2n+1)k^3, k\}$-matrix-valued differentiable function Ψ on P such that Ψ coincides with Φ_i on $p^{-1}(W_i)$ for V_i in $\mathcal{B}_j$. Let then $\Psi_1, \cdots, \Psi_{n+1}$ be the $(n+1)$ functions thus constructed. Consider a differentiable partition of unity with respect to the covering $\{D_j\}$ consisting of non-negative differentiable functions ζ_i invariant under the action of the group $U(k)$ such that the support of $\zeta_i \subset D_i$ and $\sum \zeta_i^2 = 1$.

Consider now the map Φ on P defined by

$$\Phi(\xi) = \begin{pmatrix} \zeta_1(\xi)\Psi_1(\xi) \\ \vdots \\ \zeta_{n+1}(\xi)\Psi_{n+1}(\xi) \end{pmatrix} \text{ for every } \xi \in P.$$

We have to prove that Φ is bundle map of P into $V(m,k)$ such that $\Phi^* d\Phi = \alpha$. But

$$\begin{aligned} \Phi^*\Phi(\xi) &= \sum_{i=1}^{n+1} \zeta_i(\xi)^2 \Psi_i^*(\xi)\Psi_i(\xi) \\ &= \sum \zeta_i(\xi)^2 \Psi_i^*(\xi)\Psi_i(\xi), \end{aligned}$$

the summation being over those i's for which $\xi \in D_i$. But on D_i, $\Psi_i^*\Psi_i = I$ and we have $(\Psi_i^*\Psi_i) = I$ for every i over which the summation extends. Hence $\Phi^*\Phi(\xi) = \sum \zeta_i(\xi)^2 I = I$, since $\sum \zeta_i^2(\xi) = 1$. Moreover

$$\begin{aligned} \Phi(\xi s) &= \begin{pmatrix} \zeta_1(\xi s)\Psi_1(\xi s) \\ \vdots \\ \zeta_{n+1}(\xi s)\Psi_{n+1}(\xi s) \end{pmatrix} = \begin{pmatrix} \zeta_1(\xi)\Psi_1(\xi)s \\ \vdots \\ \zeta_{n+1}(\xi)\Psi_{n+1}(\xi)s \end{pmatrix} \\ &= \begin{pmatrix} \zeta_1(\xi)\Psi_1(\xi) \\ \vdots \\ \zeta_{n+1}(\xi)\Psi_{n+1}(\xi) \end{pmatrix} s \\ &= \Phi(\xi)\cdot s \end{aligned}$$

for every $\xi \in P$ and $s \in U(k)$.

Finally,

$$\begin{aligned} \Phi^* d\Phi &= \sum_{i=1}^{n+1} \zeta_i \Psi_i^* (d\zeta_i \Psi_i + \zeta_i d\Psi_i) \\ &= \sum_{i=1}^{n+1} \Psi_i^* \Psi_i \zeta_i d\zeta_i + \sum_{i=1}^{n+1} \zeta_i^2 \Psi_i^* d\Psi_i. \end{aligned}$$

As before, for a $\xi \in P$, the summation needs to be taken only over those i's for which $\xi \in D_i$. In every such D_i, however, $\Psi_i^*\Psi_i = I$ and $\Psi_i^* d\Psi_i = \alpha$. Hence $\Phi^* d\Phi = \sum \zeta_i d\zeta_i I + (\sum \zeta_i^2)\alpha = \alpha$ since $\sum \zeta_i d\zeta_i = \frac{1}{2} d(\sum \zeta_i^2) = 0$.

5. Universal connections for compact Lie groups. Let G_2 be a closed subgroup of a Lie group G_1, and $\mathfrak{g}_2$ and $\mathfrak{g}_1$ their Lie algebras. The group G_2 acts on $\mathfrak{g}_1$ by the adjoint operations and $\mathfrak{g}_2$ is invariant under this representation. Suppose $\mathfrak{m}$ is a subspace of $\mathfrak{g}_1$ invariant under the action of G_2 which is supplementary to $\mathfrak{g}_2$. (Such a space $\mathfrak{m}$ exists if G_2 is compact or semi-simple.) Let P be a principal bundle with group G_1 and ω_1 a connection on P. P is fibred by G_2 into a principal bundle with group G_2.

The direct sum decomposition $\mathfrak{g}_2 \oplus \mathfrak{m}$ of $\mathfrak{g}_1$ gives rise to a projection π of $\mathfrak{g}_1$ onto $\mathfrak{g}_2$ which commutes with the action of G_2 (i. e. $\pi \circ ads = ads \circ \pi$ for every $s \in G_2$). We define a differential form ω_2 on P by setting $\omega_2 = \pi \circ \omega_1$. It is easy to see that ω_2 is a connection on P for the fibration by G_2. In fact, (with the notations of § 2),

$$\begin{aligned} \omega_2(X_\xi s) &= (\pi \cdot \omega_1)(X_\xi s) \\ &= \pi \cdot \omega_1(X_\xi s) \\ &= \pi \cdot \mathrm{ad}s\, \omega_1(X_\xi) \\ &= \mathrm{ad}s \cdot \pi\omega_1(X_\xi) \\ &= s^{-1}\omega_2(X_\xi)s \end{aligned}$$

for every vector X_ξ at $\xi \in P$ and $s \in G_2$.

On the other hand, for every $\xi \in P$ and $a \in \mathfrak{g}_2$, we have

$$\begin{aligned} \omega_2(\xi a) &= (\pi \cdot \omega_1)(\xi a) \\ &= \pi \cdot \omega_1(\xi a) \\ &= \pi(a) \\ &= a, \text{ since } \pi \text{ is a projection.} \end{aligned}$$

THEOREM 2. *Let G be a compact Lie group and n a positive integer. There exist a principal G-bundle B and a connection form γ_1 on B such that for every principal G-bundle P with base of dimension $\leq n$ and any connection form γ on P, one can find a bundle homomorphism f of P into B such that the inverse image of γ_1 by f is γ.*

Proof. G can be identified with a closed subgroup of a unitary group $U(k)$. Let γ_0 be a universal connection for $U(k)$ (for the dimension n) on a principal $U(k)$-bundle B, whose existence has been proved in Theorem 1. G acts on B and makes of it a principal G-bundle. One can define a connection γ_1 on this bundle by setting $\gamma_1 = \pi \circ \gamma_0$ where π is a projection of $\mathfrak{u}(k)$ onto the Lie algebra $\mathfrak{g}$ of G, as explained above. For any principal G-bundle P, with base of dimension $\leqq n$, let P' be the corresponding principal $U(k)$-bundle obtained by enlarging the group G. Then there is a natural inclusion $i \colon P \to P'$ such that $i(\xi s) = i(\xi)(s)$ for $\xi \in P$ and $s \in G$.

Moreover, if γ is a connection form on P, one can define a natural connection γ' on P' such that the inverse image of γ' by i is γ ([3], p. 35). Let Φ be a bundle map of P into B such that the inverse image of γ_0 by Φ is γ'. We define a bundle map f of P into B fibred by G by setting $f = \Phi \cdot i$. The inverse image of γ_0 by $f = \Phi \cdot i$ is obviously γ. But since γ has values in $\mathfrak{g}$ and π is identity on $\mathfrak{g}$, we have $\pi \cdot \gamma = \gamma$ and hence the inverse image of γ_1 by f is γ.

6. Remarks.

i) We show how A. Weil's theorem on connections can be deduced from our results, at least when G is compact. Let ω_1, ω_2 be two connections on a principal G-bundle P with base X of dimension $\leqq n - 1$. Consider the bundle $P \times I' \to X \times I'$ where I' is the open interval $(-\epsilon, 1 + \epsilon)$, $\epsilon > 0$. Let α_1, α_2 be inverse images of ω_1, ω_2 respectively under the projection $P \times I' \to P$. The differential form $\alpha = t\alpha_1 + (1 - t)\alpha_2$ where t is the projection $P \times I' \to I'$, is easily seen to be a connection on $P \times I'$. Let B be a principal G-bundle over a manifold M and γ_1 a universal connection on B for dimension $\leqq n$. It follows that there exists a differentiable family F_t of differentiable bundle maps of P into B such that the inverse image of γ_1 by F_t is $t\omega_1 + (1 - t)\omega_2$. If f_t are the corresponding maps of X into M, then f_0 and f_1 are obviously homotopic. On the other hand, if K_1 and K_2 are the curvature forms of ω_1, ω_2 respectively, the 'substitution' of K_1, K_2 in each polynomial over $\mathfrak{g}$ invariant under the adjoint representation of G yields closed differential forms β_1, β_2 on X. Then β_1 and β_2 are the inverse images under f_0 and f_1 of the form on M obtained by substituting the curvature form K of the universal connection in the same polynomial. Since f_0 and f_1 are homotopic, it follows that β_1 and β_2 define the same cohmology class on the base, a characteristic class of the bundle.

ii) Our method gives a universal connection for the orthogonal group $O(k)$ in particular. But the connection was defined in the complex Stiefel manifold fibred by $O(k)$ instead of the more usual real Stiefel bundle. We have already remarked (§ 2) that if the points of the real Stiefel manifold $W(N, k)$ are represented by (N, k)-matrices A satisfying $A'A = I_k$ (A' being the transpose of A), a connection can be defined in a canonical way on the real Stiefel bundle with the corresponding connection form $A'dA$. On the other hand, the complex Stiefel manifold $V(N,k)$ may be imbedded into the real Stiefel manifold $W(2N,k)$ by associating to each (N,k) matrix A, the $(2N,k)$ real matrix $\tilde{A}=\begin{pmatrix}\mathrm{Rl}\ A\\ \mathrm{Im}\ A\end{pmatrix}$ where $\mathrm{Rl}\,A$, $\mathrm{Im}\,A$ are the real and imaginary parts of A. It is easy to see that if $A^*A=I_k$, we have $\tilde{A}'\tilde{A}=I_k$. Moreover, for every $s\in O(k)\subset U(k)$

$$(\widetilde{As})=\begin{pmatrix}\mathrm{Rl}\ (As)\\ \mathrm{Im}\ (As)\end{pmatrix}=\begin{pmatrix}(\mathrm{Rl}\,A)s\\ (\mathrm{Im}\,A)s\end{pmatrix}=\tilde{A}\cdot s.$$

Hence the map $A\to\tilde{A}$ is a bundle map of the complex Stiefel manifold $V(N,k)$ fibred by $O(k)$, into the real Stiefel bundle. The connection form on $V(N,k)$ induced by this map is $\tilde{A}'d\tilde{A}$, but this is the same as the real part of A^*dA. If we take for the projection π of § 4, the map of $\mathfrak{u}(k)$ onto the Lie algebra $\mathfrak{o}(k)$ of $O(k)$ defined as the assignment of the real part to each skew Hermitian matrix, then the corresponding connection γ_1 is the same as the real part of A^*dA. In other words, the canonical connection in the real Stiefel bundle is universal for $O(k)$-bundles.

Tata Institute of Fundamental Research, Bombay.

REFERENCES.

[1] S. S. Chern, "Topics in differential geometry," *Mimeographed Notes, The Institute for Advanced Study*, Princeton, 1951.

[2] J. Nash, "The imbedding problem for Riemannian manifolds," *Annals of Mathematics*, vol. 63 (1956), pp. 20-63.

[3] K. Nomizu, "Lie groups and differential geometry," *Publications of the Mathematical Society of Japan*, 1956.

STRICT ERGODICITY AND TRANSFORMATION OF THE TORUS.*

By H. Furstenberg.

Introduction. If T is a measure preserving transformation of a probability space Ω with measure μ, the ergodic theorem assures the existence almost everywhere with respect to μ of the average $\lim_{N\to\infty} N^{-1}\sum_{n=0}^{N-1} f(T^n\omega)$, where f is an integrable function. Can this statement be improved in case Ω is a compact topological space, T a suitable homeomorphism of Ω with itself, and f a continuous function on Ω? In particular, can convergence almost everywhere be replaced by convergence everywhere? In what follows we shall examine this question for the case that Ω is an r-dimensional torus. When $r = 1$, i.e. Ω is a circle, the answer is in the affirmative and the averages in question always exist (a fact implicit in the results of Denjoy [1] and van Kampen [5]). For $r > 1$, however, further restrictions must be imposed on the transformation T and part of our objective will be to exhibit a class of T for which this sharpened form of the ergodic theorem holds.

The question we are considering is closely tied up with that of the "strict ergodicity" of a transformation. A transformation T of a compact Hausdorff space Ω is strictly ergodic if it leaves invariant a unique probability measure on the borel field of Ω. This notion was first introduced in connection with the theory of dynamical systems by Kryloff and Bogoliuboff ([6]; cf. also [8], [9]). When T is a strictly ergodic transformation, then (Theorem 1.1) the limits of $N^{-1}\sum_{n=0}^{N-1} f(T^n\omega)$ necessarily exist for f continuous and all $\omega \in \Omega$, and moreover, this limit is independent of ω. In the case of a strictly ergodic transformation, these conclusions are in fact a good deal more elementary than the usual ergodic theorem. Thus it is quite natural to inquire when a transformation of a given space will be strictly ergodic.

As we will see, an important condition for the validity of some of our conclusions is that the transformation T not be homotopic to the identity transformation. This implies that the transformation T cannot be embedded in a continuous transformation group $T(t)$ and so, in particular, could not arise from the consideration of dynamical systems on the torus. The homotopy condition also implies that the transformation is not "uniformly almost periodic," and the sample sequences $\xi(n) = f(T^n\omega)$ provide us with new classes of "constructible" sequences possessing mean values without being almost periodic in the sense of Bohr or Besicovitch.

---

* Received January 19, 1961.

A related problem is that of determining whether the space Ω is "minimal" for the transformation T. A closed invariant set is minimal for T if no proper closed subset is invariant under T. In the situation we shall study, the transformation T will also possess this irreducibility property; that is, Ω will be a minimal set. It will appear that the hypotheses required for minimality and for strict ergodicity are very similar, although not quite identical.

1. Preliminaries.

1.1. Let Ω be a compact metric space, $C(\Omega)$ its algebra of continuous complex valued functions, and T a 1-1 continuous transformation of Ω onto itself. If f is a function on Ω we shall denote by Tf the function satisfying $Tf(\omega) = f(T\omega)$. There always exists some probability meause μ on the borel field of Ω invariant under T. This follows from a general fixed point theorem regarding transformations of a compact convex set. It can also be seen by choosing a countable dense set of functions $\{f_k\}$ in $C(\Omega)$, a point $\omega \in \Omega$, and a sequence N_j such that $\lim_{j\to\infty} N_j^{-1} \sum_{n=0}^{N_j-1} f_k(T^n\omega)$ exists for all k. It follows then that this limit exists for all $f \in C(\Omega)$ and this defines a linear functional L on $C(\Omega)$. L is non-negative for non-negative function, 1 for the function 1, and $L(Tf) = L(f)$. It follows from the Riesz-Markoff representation theorem that L defines an invariant measure.

Definition 1. A continuous transformation T of Ω is called *strictly ergodic* if there is a unique probability measure on the borel field of Ω satisfying $\mu(\Delta) = \mu(T^{-1}\Delta)$ for every borel set Δ in Ω.

We remark that this definition, which is that of ([6]), differs slightly from the more current usage as in [8] and [9]. In the latter, what we have defined is referred to as "unique ergodicity," and a transformation is strictly ergodic only if in addition, the support of the unique invariant measure is all of Ω. Since the support of an invariant measure is a closed invariant set, this means that Ω is required to be a minimal set.

Given a probability measure μ on Ω, then a measure preserving transformation is ergodic in the usual sense if all borel subsets invariant under T have measure either 0 or 1. This is equivalent to saying that no probability measure absolutely continuous with respect to μ is invariant, other than μ itself. It follows that if T is a strictly ergodic transformation on Ω, it is a fortiori ergodic in the usual sense, relative to the unique invariant measure. The set of all probability measures on Ω invariant under T form a compact convex set, and one may verify that the extremal points of this set are just the ergodic measures for T, i. e. the measures with respect to which T is ergodic. Hence to show that a transformation is strictly ergodic, it suffices to show that there is a unique ergodic measure for the transformation.

We shall refer to the triple (Ω, T, μ) when μ is a probability measure on Ω invariant under T, as a *process*. If we were to fix a function $z(\omega)$ on Ω, then the functions $T^n z(\omega)$ would form a stationary stochastic process. When T is ergodic or strictly ergodic we shall refer to the process as ergodic or strictly ergodic.

Definition 2. A point $\omega \in \Omega$ is a *generic* point for the process (Ω, T, μ), if $\lim N^{-1} \sum_{n=0}^{N-1} f(T^n \omega)$ exists for every $f \in C(\Omega)$, and coincides with $\mu(f) = \int_\Omega f(\omega)\, d\mu(\omega)$.

Note that this definition differs slightly from that given in [2] where it is required in addition that ω lie in the support of the measure μ.

When a process is ergodic it follows from the ergodic theorem that almost every point of Ω is generic. For strictly ergodic processes we have ([9]):

THEOREM 1.1. *The following statements for a process (Ω, T, μ) are equivalent:*

(A) *(Ω, T, μ) is strictly ergodic.*

(B) *$N^{-1} \sum_{n=0}^{N-1} T^n f(\omega)$ converges uniformly to $\mu(f)$.*

(C) *Every point of Ω is generic for (Ω, T, μ).*

Proof. (A) implies (B): If μ is the only probability measure on Ω invariant under T, it follows that the only signed measures invariant under T are $\lambda\mu$, λ real. Hence the uniform closure in $C(\Omega)$ of the subspace $\{Tg - g, g \in C(\Omega)\}$ has codimension 1. Consequently, for any $f \in C(\Omega)$ and $\epsilon > 0$, we can find a $g \in C(\Omega)$ with $|f - \mu(f) - (Tg - g)| < \epsilon$. Hence

$$\left| \sum_0^{N-1} T^n f(\omega) - N\mu(f) - (T^N g - g) \right| < N\epsilon \text{ and } N^{-1} \sum_{n=0}^{N-1} T^n f \to \mu(f)$$

uniformly.

That (B) implies (C) is clear so it remains to show that (C) implies (A).

However, if every point of Ω is generic for (Ω, T, μ), then $N^{-1}\sum_{n=0}^{N-1} T^n f(\omega)$ converges pointwise to $\mu(f)$, and hence $\int N^{-1}\sum_{n=0}^{N-1} T^n f(\omega)\,dv(\omega) \to \mu(f)$ for any probability measure v. In particular if v is invariant under T, then $v(f) = \int N^{-1}\sum_{n=0}^{N-1} T^n f(\omega)\,dv(\omega)$ so that $v(f) = \mu(f)$.

1.2. The best known examples of strictly ergodic processes are those arising from almost periodic transformation.

Definition 3. A transformation T of Ω is *almost periodic* (a.p.) if T leaves no proper ($\neq \emptyset$ or Ω) closed subset of Ω invariant and if the powers T^n form an equicontinuous family of transformation with respect to the metric on Ω. A process (Ω, T, μ), with T almost periodic, will be referred to as an *almost periodic process.*

By the *sample paths* or *sample sequences* of a process (Ω, T, μ), we shall understand the sequences of the form $\xi(n) = T^n f(\omega)$ where $f \in C(\Omega)$. One shows easily that the sample paths of an almost periodic process are (uniformly) almost periodic sequences.

The following result appears in [8]:

THEOREM 1.2. *Every almost periodic transformation is strictly ergodic.*

Proof. The equicontinuity of the T^n implies the equicontinuity of $\{T^n f\}$ for $f \in C(\Omega)$ and hence also the equicontinuity of the averages $\{N^{-1}\sum T^n f\}$. It follows that some subsequence converges uniformly; say the limit function is g. Clearly $Tg = g$ and since T leaves no proper closed subset of Ω invariant it follows that g is a constant. Hence for any probability measure μ, $N^{-1}\sum \mu(T^n f) \to g$ and if μ is invariant, $\mu(f) = g$. Hence T is strictly ergodic.

1.3. To illustrate the general approach to the problem, we begin by examining the case in which Ω is the circle, even though the results here follow from known results regarding transformations of the circle.

THEOREM 1.3. *If T is any* 1-1 *continuous transformation of the circle such that no power of T has a fixed point, then T is strictly ergodic.*

Proof. Let K denote the circle. The hypothesis that no power of T has a fixed point, or equivalently, that T leaves no finite subset of K invariant, implies that any invariant measure must assign measure 0 to individual points, that is, any invariant measure on K is non-atomic. Let ω_0 be a fixed point on K and for two points $\omega_1, \omega_2 \in K$, let $\{\omega_1, \omega_2\}$ denote the open arc from ω_1 to ω_2 taken counterclockwise. Suppose that μ and μ' are two invariant probability measures on K and let $\lambda = \frac{1}{2}(\mu + \mu')$. We define a map Φ from K to a circle K' by setting $\Phi(\omega) = e^{2\pi i\lambda(\{\omega_0,\omega\})}$. Since λ is non-atomic, Φ will be a continuous map from K onto K'.

We note that for any three points ω_1, ω_2, ω_3 in K,

$$\lambda(\{\omega_1,\omega_2\}) + \lambda(\{\omega_3,\omega_3\}) \equiv \lambda(\{\omega_1,\omega_3\}) \pmod 1.$$

It follows that

$$\Phi(T\omega) = e^{2\pi i\lambda(\{\omega_0,T\omega\})} = e^{2\pi i[\lambda(\{\omega_0,T\omega\}) + \lambda(T\{\omega_0,T\omega\})]}$$

$$= e^{2\pi i a}e^{2\pi i\lambda(\{T\omega_0,T\omega\})} = e^{2\pi i a}e^{2\pi i\lambda(\{\omega_0,\omega\})} = e^{2\pi i a}\Phi(\omega)$$

where $\alpha = \lambda(\{\omega_0, T\omega_0\})$. If α were rational we would have $\Phi(T^n\omega) = \Phi(\omega)$ identically for some n. Then $\lambda(\{\omega_0, T^n\omega\} \equiv \lambda(\{\omega_0,\omega\}) \pmod 1$ so that $\lambda(\{\omega, T^n\omega\}) \equiv 0 \pmod 1$ and the interval from ω to $T^n\omega$ carries either measure 0 or 1. Thus either $\lambda(\{\omega, T^n\omega\}) = 0$ or $\lambda(\{T^n\omega,\omega\}) = 0$ and whichever holds for some ω and $T^n\omega$ and it follows that every interval of sufficiently small length on K carries no λ measure. This however is impossible since $\lambda \neq 0$ and this shows that α is irrational.

Thus Φ carries λ into (normalized) lebesgue measure on K' and it takes T into the rotation of K' by an irrational angle. Now μ and μ' are carried by Φ into two measures on K' that are invariant under rotation by an irrational angle, since μ and μ' are invariant under T. But clearly the rotations of a circle preserving a given measure form a closed group. (If $\beta_n \to \beta$ and f is continuous then $f(\theta + \beta_n) \to f(\theta + \beta)$ and $\int f(\theta + \beta_n)dV(\theta) \to \int f(\theta + \beta)dV(\theta)$.) Hence μ and μ' are carried into probability measures on K' invariant under all rotations, i. e. into lebesgue measure. Thus μ and μ' have the same images under Φ. On the other hand, if two intervals of K map onto the same interval of K' under Φ, their symmetric difference carries 0 λ-measure. A fortiori it carries 0 μ- and μ'-measure, and so both intervals have the same μ-measure and μ'-measure. It follows that the measures μ and μ' are determined by their images under Φ and since these agree, $\mu = \mu'$. This proves that T is strictly ergodic.

COROLLARY. *If T is any continuous transformation of the circle, then* $\lim N^{-1}\sum_{n=0}^{N-1} T^n f(\omega)$ *exists for all continuous functions f and points ω on the circle.*

Proof. If no power of T has a fixed point then the result follows from Theorems 1.1 and 1.3. If some T^m has a fixed point, let $T_1 = T^m$. It is easily shown then that for every point ω, $T_1{}^n\omega$ converges to a fixed point of T_1. Therefore the averages $\lim N^{-1}\sum_{n=0}^{N-1} T_1{}^n f(\omega)$ exist for all ω. Applying this to the functions $f, Tf, \cdots, T^{m-1}f$ we conclude that $\lim N^{-1}\sum_{n=0}^{N-1} T^n f(\omega)$ exists.

In case T leaves no proper closed subset of K invariant, then the support of the unique invariant measure λ must be all of K. The map Φ of Theorem 1.3 is then a homeomorphism and we can say that the process (K, T, λ) is equivalent to the process induced by an irrational rotation of the circle. In particular the process (K, T, λ) is almost periodic and the sample paths are almost periodic sequences with frequencies $k\alpha$.

2. Processes on the torus.

2.1. The following lemma provides us with an inductive procedure for defining strictly ergodic processes.

LEMMA 2.1. *Let* (Ω_0, T_0, μ_0) *be a strictly ergodic process, let* K *be the circle,* $K = \{\zeta : |\zeta| = 1\}$, *and let* m *be (normalized) lebesgue measure on* K. *Take* $\Omega = \Omega_0 \times K$ *and* $T : \Omega \to \Omega$ *defined by* $T(\omega_0, \zeta) = (T_0\omega_0, g(\omega_0)\zeta)$ *where* $g(\omega_0)$ *is a continuous function with* $|g| = 1$. *Then* T *is a strictly ergodic transformation if and only if the equation*

$$g^k(\omega_0) = R(T_0\omega_0)/R(\omega_0) \tag{1}$$

has no solution for k *an integer* $\neq 0$ *and* $R(\omega_0)$ *a measurable function on* (Ω_0, μ_0). *In any case, the product measure* $\mu_0 \times m$ *is an invariant measure for* T.

Proof. To verify that $\mu_0 \times m$ is an invariant measure, set $f(\omega) = f_1(\omega_0)f_2(\zeta)$. Then $Tf(\omega) = T_0f_1(\omega_0)f_2(g(\omega_0)\zeta)$ and

$$\begin{aligned}
\int_\Omega Tf(\omega)\,d\mu \times m(\omega) &= \int_{\Omega_0}\Big[\int_K f_2(g(\omega_0)\zeta)\,dm(\zeta)\Big]T_0f_1(\omega_0)\,d\mu_0(\omega_0)\\
&= \int_{\Omega_0}\Big[\int_K f_2(\zeta)\,dm(\zeta)\Big]T_0f_1(\omega_0)\,d\mu_0(\omega_0)\\
&= \int_K f_2(\zeta)\,dm(\zeta)\int_{\Omega_0} f_1(\omega_0)\,d\mu_0(\omega_0)\\
&= \int_\Omega f(\omega)\,d\mu \times m(\omega).
\end{aligned}$$

We claim that in order that T be strictly ergodic on Ω it suffices that it be ergodic in the ordinary sense with respect to $\mu = \mu_0 \times m$. To see this define the transformation $S_\beta : \Omega \rightarrow \Omega$ by $S_\beta(\omega, \zeta) = (\omega_0, e^{2\pi i\beta}\zeta)$. Clearly S_β preserves the measure μ. It follows easily that if ω is a generic point for (Ω, T, μ) then so is $S_\beta(\omega)$ for every $\beta \in [0, 1)$. Now suppose that T is ergodic with respect to μ. Then almost all points of Ω (with respect to μ) are generic for (Ω, T, μ). Hence for almost all ω_0 (with respect to μ_0), *all* points (ω_0, ζ) are generic for (Ω, T, μ). Suppose next that there exists some other ergodic measure μ' for T. Since a T-invariant measure on Ω induces a T_0-invariant measure on Ω_0 in a natural way, and since (Ω_0, T_0, μ_0) is strictly ergodic, μ' must induce the same measure μ_0 on Ω_0. Then for almost all ω_0 in Ω_0 there exist points (ω_0, ζ) generic for (Ω, T, μ'). But this is impossible if $\mu' \neq \mu$, since for almost all ω_0, all (ω_0, ζ) are generic for (Ω, T, μ). Thus if $\mu = \mu_0 \times m$ is ergodic, it is the unique ergodic invariant measure and hence the unique invariant measure (cf. the remarks following Definition 1).

To determine whether μ is ergodic, suppose that $Tf = f$ where $f \in L^2(\Omega, \mu)$. Since μ is a product measure we can write $f \sim \sum_{-\infty}^{\infty} c_k(\omega_0)\zeta$ with $c_k(\omega_0) \in L^2(\Omega_0, \mu_0)$. $Tf = f$ implies $\sum_{-\infty}^{\infty} c_k(T_0\omega_0)g^k(\omega_0)\zeta^k = \sum_{-\infty}^{\infty} c_k(\omega_0)\zeta^k$ or $c_k(T_0\omega_0) = g^{-k}(\omega_0)c_k(\omega_0)$ for every k. Since T_0 is ergodic, f cannot reduce to a function of ω_0 alone and hence some $c_k(\omega_0)$ is not 0 for $k \neq 0$. Since $|g| = 1$ it follows from the ergodicity of T_0 that c_k vanishes only on a set of measure 0, so that $R(\omega_0) = c_k(\omega_0)^{-1}$ is a solution of (1).

Conversely, if (1) has a solution, then the function $R(\omega)\zeta^{-k}$ is invariant under T so that μ is not ergodic. This completes the proof of the lemma.

We note that if (1) has a solution $R(\omega_0)$, then $|R(\omega_0)|$ is almost everywhere constant and we may assume that $|R(\omega_0)| = 1$.

2.2. If ϕ is a map from a topological space to the circle K then ϕ is called *essential* if it is not homotopic to the constant map, or equivalently if ϕ does not have a single-valued continuous logarithm. When the space is the circle then the increase in $\frac{1}{2\pi i}\log\phi(\zeta)$ as ζ describes the circle once is an integer referred to as the *degree* of ϕ. Thus ϕ is essential if and only if its degree does not vanish.

Lemma 2.1 provides us with strict ergodicity in case the function $g(\omega_0)$ on Ω_0 satisfies a certain condition with respect to T_0. In the next lemma we find a particular form for (Ω_0, T_0) and $g(\omega_0)$ so that the condition is satisfied. Here Ω_0 is itself the product of a space Ω_1 and the circle, and the points ω_0 of Ω_0 may be represented as (ω_1, ζ), $\omega_1 \in \Omega_1$, $\zeta \in K$.

LEMMA 2.2. *Let* $\Omega_0 = \Omega_1 \times K$ *where* Ω_1 *is a connected metric space, let*

μ_1 be a probability measure on Ω_1, Ω, and T_1 a continuous measure preserving transformation of Ω_1. Suppose that T_0: Ω_0 is given by $T_0(\omega_1, \zeta) = (T_1\omega_1, q(\omega_1)\zeta)$ and that T_0 is ergodic with respect to the measure $\mu_1 \times m = \mu_0$ on Ω_0. Let $g(\omega_1, \zeta)$ be a continuous function on Ω_0 such that $g(\omega_1, \zeta)$ is an essential map of $K \to K$ for fixed ω_1 and satisfying a uniform Lipschitz condition in ζ:

$$|g(\omega_1, \zeta') - g(\omega_1, \zeta'')| < M\,|\zeta' - \zeta''|.$$

Then equation (1), $g^k(\omega_0) = R(T_0\omega_0)/R(\omega_0)$, has no solution for $k \neq 0$ and $R(\omega_0)$ measurable on (Ω_0, μ_0).

Proof. Since Ω_1 is connected, the degree d of the map $g: \omega_1 \times K \to K$ is independent of ω_1, and, in particular, if the map is essential for one ω_1, is is so for all. The degree of g^k will be kd and so g^k is again essential in its second variable and also satisfies a uniform Lipschitz condition. Thus to prove the lemma it suffices to show that $g(\omega_0)$ itself cannot have the form $R(T_0\omega_0)/R(\omega_0)$ with $R(\omega_0)$ a measurable function from Ω to K.

Note that if $d(.,.)$ is a metric for Ω_1, then $d((\omega_1', \zeta'), (\omega_1'', \zeta'')) = \max(d(\omega_1', \omega_1''), |\zeta' - \zeta''|)$ is a metric on Ω_0. Now suppose that $g(\omega_0) = R(T_0\omega_0)/R(\omega_0)$. Since R is a measurable function it is continuous when restricted to some compact subset of Ω_0 with measure $> 1 - \eta$, for arbitrary $\eta > 0$. Hence for a specified δ, $\delta' > 0$, there exists an $\epsilon > 0$ and a subset Λ of Ω with $\mu_0(\Lambda) > 1 - \delta$ and such that $|R(\omega_0') - R(\omega_0'')| < \delta'$ whenever $d(\omega_0', \omega_0'') < \epsilon$ and $\omega_0'\,\omega_0'' \in \Lambda$. We set

$$\Lambda_1 = \{\omega \in \Omega_1 : m(\zeta : (\omega_1\,\zeta) \in \Lambda) \geqq 1 - \delta^{\frac{1}{2}}\}.$$

Then $\Lambda_1 \subset \Omega_1$ and $\mu_1(\Lambda_1) \geqq 1 - \delta^{\frac{1}{2}}$.

If $\delta < 1$, then Λ_1 and hence $\Lambda_1 \times K$ will have positive measure. Therefore there will exist $\epsilon/2$-neighborhoods in Ω_0 intersecting $\Lambda_1 \times K$ in sets of positive measure; let V be such a neighborhood. By the ergodicity of $\mu_0 = \mu_1 \times m$, there will exist points in $V \cap (\Lambda_1 \times K)$ such that infinitely many of their images under T_0^n again lie in $V \cap (\Lambda_1 \times K)$. Let (ω_1', ζ') be such a point and suppose that $T_0^{n_k}(\omega_1', \zeta') \in V \cap (\Lambda_1 \times K)$.

Now define $S_\beta: \Omega_0 \to \Omega_0$ as in Lemma 2.1; i.e. $S_\beta(\omega_1, \zeta) = (\omega_1, e^{2\pi i\beta}\zeta)$. From the definition of T_0, it is easily checked that each S_β commutes with T_0. Moreover S_β preserves the metric $d(.,.)$ in Ω_0. By applying S_β to (ω_1', ζ') we find that for all ζ, $d(T_0^{n_k}(\omega_1', \zeta), (\omega_1', \zeta)) < \epsilon$, and both (ω_1', ζ) and $T^{n_k}(\omega_1', \zeta)$ lie in $\Lambda_1 \times K$.

From the definition of T_0 we find that $T^{n_k}(\omega_1', \zeta) = (T_1^{n_k}\omega_1', e^{2\pi i\beta_k}\zeta)$ where β_k is independent of ζ. Now since (ω_1', ζ) and $T^{n_k}(\omega_1', \zeta)$ lie in $\Lambda_1 \times K$, it follows that the set of ζ for which the former is not in Λ has measure $< \delta^{\frac{1}{2}}$, and similarly for the latter. Since the ζ's for the two points are fixed translates of one another it follows that the set of ζ such that either (ω_1', ζ) or $T_0^{n_k}(\omega_1', \zeta)$ is not in Λ has measure $< 2\delta^{\frac{1}{2}}$. Putting all this together we conclude that but for a set of ζ of measure $< 2\delta^{\frac{1}{2}}$,

$$| R(T_0^{n_k}(\omega_1', \zeta)) - \mathrm{R}(\omega_1', \zeta) | < \delta'.$$

To complete the proof of the lemma we observe that $| R(T_0^{n_k}\omega) - R(\omega) | < \delta'$ implies that $| g(T_0^{n_k-1}\omega) \cdots g(T_0\omega) g(\omega) - 1 | < \delta'$. Now we may write $g(T_0^j(\omega_1', \zeta)) = g(T_1^j\omega_1', e^{2\pi i\alpha_j}\zeta) = e^{2\pi i h_j(\theta)}$ where $\zeta = e^{2\pi i\theta}$. Since g satisfies a uniform Lipschitz condition in ζ it follows that the $h_j(\theta)$ satisfy uniformly a Lipschitz condition: $| h_j(\theta_1) - h_j(\theta_2) | < M | \theta_1 - \theta_2 |$. Since g is essential in ζ we will have $h_j(\theta + 1) = h_j(\theta) + d$ where $d \neq 0$ is the degree of g. Set $H_k(\theta) = \sum_{j=0}^{n_k-1} h_j(\theta)$; then $H_k(\theta + 1) = H_k(\theta) + n_k d$ and $| H_k(\theta_1) - H_k(\theta_2) | < M n_k | \theta_1 - \theta_2 |$.

We have then $| e^{2\pi i H_k(\theta)} - 1 | < \delta'$ for all θ outside a set of θ of measure $< 2\delta^{\frac{1}{2}}$. Taking $\delta' \leqq \sqrt{2}$ implies that $H_k(\theta)$ has to remain within a distance $\frac{1}{4}$ from an integer, for all θ outside of a set of measure $< 2\delta^{\frac{1}{2}}$. But $H_k(\theta)$ is a continuous function, and as θ goes from 0 to 1, $H_k(\theta)$ has a range of length at least $n_k d$. This implies that in the exceptional set of measure $< 2\delta^{\frac{1}{2}}$, $H_k(\theta)$ oscillates by $\geqq \frac{1}{2} n_k d$. But by the Lipschitz condition, in a set of measure $< 2\delta^{\frac{1}{2}}$, $H_k(\theta)$ can oscillate by at most $2Mn_k\delta^{\frac{1}{2}}$, and this gives a contradiction if $\delta < (\frac{d}{4M})^2$, which proves the lemma.

Note that the lemma is true, in particular, when Ω_1 reduces to a single point so that Ω_0 is just the circle K.

2.3 THEOREM 2.1. *Let T be a transformation of $\Omega = K^r$ given by*

$$\begin{aligned} T\zeta_1 &= e^{2\pi i\alpha}\zeta_1 \\ T\zeta_2 &= g_1(\zeta_1)\zeta_2 \\ &\cdots \\ T\zeta_{j+1} &= g_j(\zeta_1, \cdots, \zeta_j)\zeta_{j+1} \qquad (2) \\ &\cdots \\ T\zeta_r &= g_{r-1}(\zeta_1, \cdots, \zeta_{r-1})\zeta_r \end{aligned}$$

where α is irrational, each g_j is a continuous function with $| g | = 1$, each $g_j(\zeta_1, \cdots, \zeta_j)$ satisfies a uniform Lipschitz condition in ζ_j, and $g_j(\zeta_1, \cdots, \zeta_j)$ is of degree d_j in ζ_j where $d_j \neq 0$. Then T is a strictly ergodic transformation and the unique invariant measure is the normalized lebesgue measure on K^r.

Proof. The theorem is valid for $r = 1$ by virtue of Theorem 1.2 or Theorem 1.3. Now assume the theorem is valid for $\Omega = K^{r-1}$. By Lemma 2.1 it will follow for $\Omega = K^r$ if the equation

$$g_{r-1}^{k}(\omega_0) = R(T_0\omega_0)/R(\omega_0)$$

has no measurable solution, where T_0 is the induced transformation on K^{r-1} and $\omega_0 \in K^{r-1}$. But the space K^{r-1} has the form $K^{r-2} \times K$ and T_0 is induced by T_1 on K^{r-2} in the manner prescribed in Lemma 2.2. Since the hypotheses of Lemma 2.2 are fulfilled, it follows that the equation in question has no solution. The theorem therefore follows by induction on r.

If we denote the invariant probability measure on K^r by μ, we notice that for $i \neq j$, $\mu(\phi(\zeta_i)\psi(\zeta_j)) = \mu(\phi(\zeta_i))\mu(\psi(\zeta_j))$, so that for $i \neq j$, ζ_i and ζ_j are independent variables. Taking $j = 1$ we obtain in particular

$$\lim N^{-1} \sum_{n=0}^{N-1} T^n \zeta_1{}^l(\omega) T^n \phi(\zeta_i)(\omega) = \mu(\zeta_1{}^l)\mu(\phi(\zeta_i)) = 0$$

if $l \neq 0$. Since $T^n \zeta_1{}^l = e^{2\pi i n l \alpha} \zeta_1{}^l$ this says that the Bohr-Fourier coefficients of the sample sequence $T^n \phi(\zeta_i)(\omega)$ corresponding to the frequencies $l\alpha$ all vanish. Now Theorem 2.1 easily extends to the case where the base process $(T\zeta_1 = e^{2\pi i \alpha} \zeta_1)$ is replaced by any almost periodic process. This implies that for any $\phi(\zeta_i)$, $i \neq 1$, the corresponding sample sequences have all their Bohr-Fourier coefficients vanishing except for the constant term. In particular, the sample sequences are not all uniformly almost periodic (or, for that matter, even Besicovitch almost periodic). Hence the transformation T itself cannot be almost periodic. That this is the case could have been deduced from the fact that neither T nor any power of T is homotopic to the identity transformation (since the $d_j \neq 0$). But if T is almost periodic then some sequence, T^{n_j} converges uniformly to the identity, and since the homotopy classes of maps of $K^r \to K^r$ form a discrete set, this cannot happen unless eventually T^{n_j} is homotopic to the identity transformation.

Remark. Theorem 2.1 implies in particular that the transformations (2) leave no proper closed subset of K^r invariant. It should be pointed out that for this weaker conclusion one can dispense with the Lipschitz condition on the g; (but not with the condition that the $d_j \neq 0$). In fact one can prove an analogue of Lemma 2.1 with strict ergodicity replaced by the condition that no proper closed sets are invariant. Here the condition on $g(\omega_0)$ becomes that equation (1) has no solution with $R(\omega_0)$ continuous, rather than measurable. However, this is the case if $g(\zeta_1, \cdots, \zeta_i)$ is essential as a function of ζ_j. For $R(\zeta_1, \cdots, \zeta_j)$ would have a certain degree in ζ_j and one verifies from (2) that $TR(\zeta_1,\cdots,\zeta_j)$ has the same degree in ζ_j. Then $TR(\zeta_1,\cdots,\zeta_j)/R(\zeta_1,\cdots,\zeta_j)$ would have degree 0 in ζ_j and could not equal $g(\zeta_1,\cdots,\zeta_j)$ which is essential in ζ_j. Thus the smoothness condition on the g_j's in Theorem 2.1 is needed only to ensure that no measurable solution exist to (1).

2.4. The sample sequence of a strictly ergodic process not only possess averages but these averages are taken on with a certain uniformity. More precisely

$$N^{-1}\sum_{k+1}^{k+N} T^n f(\omega)\to\mu(f)$$

uniformly in k as $N\to\infty$. This is an immediate consequence of Theorem 1.1. This notion occurs in [10] and [7] in the definition of a "well-distributed" sequence. A sequence $\zeta(n)$ on the unit circle is well-distributed if $\lim_{N\to\infty} N^{-1}\sum_{k+1}^{k+N} f(\zeta(n))=\int_k f(\zeta)\,dm(\zeta)$ uniformly in k, thus strengthening the condition for equidistribution. We might observe that the theorem ([7]) that if $p(n)$ is a polynomial in n with an irrational coefficient, then $e^{2\pi i p(n)}$ is well distributed, is a consequence of Theorem 2.1. In fact, by an appropriate choice of integers ν_{ij} and a point $\omega\in K^r$, the sample sequence $T^n\zeta_r(\omega)$ will have the form $e^{2\pi i(\alpha n^r+\alpha_1 n^{r-1}+\cdots+\alpha_r)}$ if the functions g_j have the form $g_j(\zeta_1,\cdots,\zeta_j)=\zeta_1^{\nu_{j1}}\cdots\zeta_j^{\nu_{jj}}$. The "well-distribution" of $T^n\zeta_r(\omega)$ then follows from the fact that the unique stationary measure on K^r is lebesgue measure. This takes care of the case that $p(n)$ has its first coefficient irrational; the general case easily reduces to this one.

3. Existence of ergodic averages.

3.1. It is possible to show by examples that the conditions on the smoothness and the topological nature (i.e., the non-vanishing of degree) of the functions g_j occurring in Theorem 2.1 cannot be essentially weakened. For example, if the Lipschitz condition is replaced by the requirement that the g_j be of bounded variation, then the conclusion of Theorem 2.1 fails to hold, as a rather intricate construction shows. The necessity of the topological assumption is more evident since, e.g., the map: $T\zeta_1=e^{2\pi i\alpha}\zeta_1$, $T\zeta_2=e^{2\pi i\rho\alpha}\zeta_2$ of the torus K^2 is clearly not strictly ergodic if ρ is rational. In the latter case, however, the ergodic averages, $\lim N^{-1}\sum_{n=0}^{N-1} T^n f(\omega)$ still exist for all ω, although they are no longer independent of ω. We will see in this section that the hypotheses of Theorem 2.1 are still relevant for the weaker conclusion of existence everywhere of the ergodic averages.

THEOREM 3.1. *Let* (Ω_0, T_0, μ_0) *be a strictly ergodic process, let* $\Omega = \Omega_0 \times K$ *and let* $T\colon \Omega \to \Omega$ *be defined by* $T(\omega_0, \zeta) = (T_0\omega_0, g(\omega_0)\zeta)$ *where* g *is a continuous function from* Ω_0 *to* K. *Then if the equation*

$$g^k(\omega_0) = R(T_0\omega_0)/R(\omega_0) \tag{1'}$$

has a solution $R(\omega_0)$ *which is measurable but not equal almost everywhere to a continuous functions, then* $\lim N^{-1} \sum_{n=0}^{N-1} T^n f(\omega)$ *cannot exist for all continuous* f *and all* $\omega \in \Omega$.

Proof. Let $\phi(\omega)$ be a continuous function of Ω_0 with $\mu_0(\phi \cdot R) \neq 0$, and consider the expressions $T^n(\phi(\omega_0)\zeta^k)$. We have

$$T\zeta^k = g^k(\omega_0)\zeta^k = R(T_0\omega_0)R(\omega_0)^{-1}\zeta^k, \text{ or } T(\zeta^k R(\omega_0)^{-1}) = \zeta^k R(\omega_0)^{-1},$$

whence $T^n(\zeta^k R(\omega_0)^{-1}) = \zeta^k R(\omega_0)^{-1}$, so that

$$T^n(\phi(\omega_0)\zeta^k) = \zeta^k R(\omega_0)^{-1} T_0^n(\phi(\omega_0)R(\omega_0)). \tag{3}$$

Suppose now that all ergdoic everages exist for continuous functions on Ω. Then the average of the left hand side of (3) exists, and so

$$\zeta^k R(\omega_0)^{-1} \lim N^{-1} \sum_{n=0}^{N-1} T^n(\phi(\omega_0)R(\omega_0)) = \lim N^{-1} \sum_{n=0}^{N-1} T^n(\phi(\omega_0)\zeta^k) = \psi(\omega_0, \zeta)$$

is defined. Since (Ω_0, T_0, μ_0) is ergodic we have

$$\zeta^k R(\omega_0)^{-1}\mu_0(\phi \cdot R) = \psi(\omega_0, \zeta)$$

almost everywhere. Since $\mu_0(\phi \cdot R) \neq 0$ and $\psi(\omega_0, \zeta)$ is a limit everywhere of continuous functions on Ω, it follows that $R(\omega_0)$ agrees almost everywhere with a function $\bar{R}(\omega_0)$ of Baire class 1 on Ω, and hence on Ω_0. We shall show that this together with (1′) implies that $R(\omega_0)$ agrees almost everywhere with a continuous function, contrary to hypothesis.

We say that a function $f(\omega_0)$ has an essential jump $\geqq \delta$ at a point ω_0, if, for any function $\bar{f}$ equal to f a. e., $\limsup_{\omega', \omega'' \to \omega_0} |\bar{f}(\omega') - \bar{f}(\omega'')| \geqq \delta$. Thus if R is not equivalent to a continuous function, then R, and hence $\bar{R}$, must have essential jumps $\geqq \delta$ for some $\delta > 0$. Now equation (1′) still holds a. e. for $\bar{R}$ and from it we see that the set of points at which $\bar{R}$ has an essential jump $\geqq \delta$ is invariant under T_0. Moreover the set of points at which a function has an essential jump $\geqq \delta$ is closed. Now if (Ω_0, T_0, μ) is strictly ergodic, every invariant closed subset of Ω must contain the support of μ_0. Since we may assume that the support of μ_0 was all of Ω_0 it follows that $\bar{R}(\omega_0)$ has essential jumps everywhere. But by Baire's theorem, a function of the first class must have points of continuity ([4]). This proves the theorem.

If the space Ω_0 in the theorem is itself of the form $\Omega_0 = \Omega_1 \times K$ and T_0 has a form analogous to that of T, and if $g(\omega_0) = g(\omega_1, \zeta)$ is essential in ζ, then equation (1′) cannot have a continuous solution (cf. the remark in § 2. 3). Thus, if in this case the ergodic averages exist everywhere, then T must be strictly ergodic. So, in the example referred to earlier, where the g_j in Theorem 2. 1 are of bounded variation, but do not satisfy a Lipschitz condition, and the process need not be strictly ergodic, neither will the ergodic averages all exist.

Using Theorem 3. 1 we can give an example of a map T of K^2 of the form (2), where T is a C^∞ transformation, but fails to satisfy the topological hypothesis, and such that the ergodic averages do not all exist. Define a sequence of integers v_k with $v_1 = 1$ and $v_{k+1} = 2^{v_k} + v_k + 1$. Set $\alpha = \sum_{\infty}^{1} 2^{-v_k}$. Writing $n_k = 2^{v_k}$ we obtain

$$(3) \qquad |n_k\alpha - [n_k\alpha]| > \frac{2 \cdot 2^{v_k}}{2^{v_{k+1}}} = 2^{-n_k}$$

where $[x]$ denotes the largest integer not exceeding x.

Define $n_{-k} = -n_k$ and set

$$h(\theta) = \sum_{k \neq 0} \frac{1}{|k|} (e^{2\pi i n_k \alpha} - 1) e^{2\pi i n_k \theta}$$

and let $g(e^{2\pi i \theta}) = e^{2\pi i \lambda h(\theta)}$ where λ is as yet undetermined. Note that $g(\zeta)$ is inessential. By (3), $h(\theta)$ and hence $g(\zeta)$ are C^∞ functions. Now we have $h(\theta) = H(\theta + \alpha) - H(\theta)$ where

$$H(\theta) = \sum_{k \neq 0} \frac{1}{|k|} e^{2\pi i n_k \theta}$$

so that $H(\theta)$ is in $L^2(0,1)$ and, in particular, defines a measurable function. However $H(\theta)$ cannot correspond to a continuous function since $\sum \frac{1}{|k|} = \infty$ and hence the series is not Cesàro summable at $\theta = 0$ ([11]). Therefore $e^{2\pi i \lambda H(\theta)}$ will not be a continuous function for some λ. Taking $R(e^{2\pi i \theta}) = e^{2\pi i \lambda H(\theta)}$ we have

$$R(e^{2\pi i \alpha}\zeta)/R(\zeta) = g(\zeta)$$

with $R(\zeta)$ measurable but not continuous. By Theorem 3. 1, the transformation T of K^2 given by

$$T\zeta_1 = e^{2\pi i \alpha}\zeta_1, \qquad T\zeta_2 = g(\zeta_1)\zeta_2,$$

will not possess all its ergodic averages.

3.2. The transformations given by (2) are in a "triangular" form, and this, we may note, implies certain restrictions in the homotopy classes of the transformations under consideration. Fixing our attention on the case $r = 2$, we note that the induced transformation on the 1-dimensional integral homology group is given by a matrix

$$\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}$$

where d is the degree of $g(\zeta_1)$. Namely, the homology group is generated by the classes of the cycles $\rho_1 = \{\zeta_2 = 1\}$, $\rho_2 = \{\zeta_1 = 1\}$. Under the transformation

$$T\zeta_1 = e^{2\pi i}\zeta_1$$
$$T\zeta_2 = g(\zeta_1)\zeta_2 \tag{4}$$

ρ_1 is transformed into $\rho_1 + d\rho_2$ and ρ_2 into ρ_2 in the homology group. Now the homotopy classes of homeomorphisms of K^2 with itself are in one-one correspondence with the induced transformation of the first integral homology group, and so may be represented by 2×2 unimodular matrices with integer coefficients. Thus the homotopy classes that are represented by the transformations in (4) are just those whose matrices have both eigenvalues 1, or equivalently, have trace 2. Now this restriction is quite natural if we are interested in strictly ergodic transformations, since if the associated matrix does not have trace 2, the map necessarily has a fixed point. This can be shown directly as a consequence of the fact that any two cycles on K^2 that are not homologous to multiples of the same cycle, must intersect. It is also a simple corollary of the Lefschetz fixed point theorem. However, a fixed point of the transformation is clearly not generic for a process unless the process degenerates to that one point, and so in any other case, the transformation cannot be strictly ergodic.

The next theorem indicates that this restriction (with a slight modification) is also necessary for the existence of ergodic averages. We call a transformation of the torus linear if it is induced by a linear transformation of the plane. In order for this to happen, the associated matrix of the linear transformation on the plane must be a unimodular matrix with integer entries. It is easy to verify that this same matrix represents the homology class of the induced transformation of the torus.

THEOREM 3.2. *Let T be a transformation of the torus induced by the transformation*

$$x' = ax + by + x'_0$$
$$y' = cx + dy + y'_0 \tag{5}$$

of the plane R^2, *where* a, b, c, d *are integers and* $ad - bc = 1$. *Then* $\lim N^{-1} \sum_{n=0}^{N-1} T^n f(\omega)$ *exists for every continuous function* f *on* K^2 *and* $\omega \in K^2$, *if and only if* $|a + d| \leqq 2$.

Proof. If $a + d = 2$ then both eigenvalues of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ are 1 in which case, by a linear change of coordinates, (5) may be put into the form

$$\begin{aligned} x' &= x + x'_0 \\ y' &= dx + y + y'_0. \end{aligned} \tag{6}$$

If $d = 0$, or if $d \neq 0$ and x'_0 is rational, it is easily checked that the sample sequences of the induced process are periodic or almost periodic. If $d \neq 0$ and x'_0 is irrational then the ergodic averages exist by virtue of Theorem 2.1.

If $-2 \leqq a + d < 2$, then the eigenvalues of A are roots of unity and an appropriate power of A will have both eigenvalues 1. Hence a power of T will fall into the category already treated, and the existence of ergodic averages for a power of T implies the existence of these averages for T itself.

We may therefore turn to the case $|a + d| > 2$. Here we wish to show that the ergodic averages need not exist. Since in this case the induced transformation of the torus has a fixed point, we may assume that the fixed point corresponds to the origin in the plane and that T in the plane is given by

$$\begin{aligned} x' &= ax + by \\ y' &= cx + dy, \quad |a + d| > 2. \end{aligned} \tag{7}$$

We now consider T solely as a transformation of R^2. We denote by Z^2 the lattice of points of R^2 with integer coordinates, and for a set Δ in R^2, $\Delta + Z^2$ will denote the set of all points in R^2 congruent to a point in Δ modulo Z^2. We let l_1 and l_2 represent the lines through the origin containing the eigenvectors of A; l_1 will correspond to the eigenvalue λ, and l_2 to the eigenvalue λ^{-1}. Since $|\lambda + \lambda^{-1}| > 2$, λ and λ^{-1} will be real and we take $|\lambda| > 1$. Also λ is not an integer since $\lambda + \lambda^{-1}$ is, and since $\lambda^2 - (a + d)\lambda + 1 = 0$, it follows that λ is irrational. Hence the slopes of l_1 and l_2 are irrational and so the sets $l_1 + Z^2$ and $l_2 + Z^2$ are dense in R.

We consider parallelograms whose sides are respectively parallel to l_1 and l_2; we call these oriented parallelograms. The "width" of the parallelogram will denote the length of the side parallel to l_1, its "height," the length of the adjacent side. T takes one oriented parallelogram into another one, multiplying its width by $|\lambda|$ and its height by $|\lambda|^{-1}$. Let Q_1 and Q_2 be two oriented rhombuses with centers of the origin of R^2, and with sides equal to ϵ

and 2ϵ respectively. ϵ will be determined later. To prove that not all ergodic averages exist for the induced transformation of the torus we will show that there exists a point ω in R^2 with

$$\limsup_{N\to\infty} N^{-1}\{\#\text{ of points } T^n\omega,\ 0\leqq n<N,\ \text{such that } T^n\omega\in Q_1+Z^2\}$$
$$>\liminf_{N\to\infty} N^{-1}\{\#\text{ of points } T^n\omega,\ 0\leqq n<N,\ \text{such that } T^n\omega\in Q_2+Z^2\}.$$

Since $Q_1\subset Q_2$ this implies that for a doubly periodic continuous function f on R^2 that equals 1 on Q_1 and vanishes outside of Q_2, $\lim N^{-1}\sum T^n f(\omega)$ does not exist. But this implies that for the induced transformation on K^3 and the associated function on K^2, the ergodic average doesn't exist at all points.

To obtain the point ω we prove the following two statements.

(a) Given an oriented parallelogram P there exists an N_0 such that for any $N>N_0$ there is an oriented parallelogram $P_a\subset P$ with the property that for any $\omega\in P_a$, the number of times $T^n\omega\in Q_2+Z^2$ for $0\leqq n<N$, is $\leqq\beta_1\epsilon^2N$, β_1 being a constant depending only on A.

(b) Given a noriented parallelogram P there exists an N_0 such that for any $N>N_0$ there is an oriented parallelogram $P_b\subset P$ with the property that for any $\omega\in P_b$ the number of times $T^n\omega\in Q_1+Z^2$ for $0\leqq n<N$, is $\geqq(\beta_2+\beta_3\log\epsilon^{-1})^{-1}N$ where β_2 and β_3 depend only on A.

The proof of (a) depends on the fact that the transformation T on the torus is ergodic with respect to lebesgue measure (as a straightforward Fourier series argument shows). Hence for almost all $\omega\in R^2$, the frequency of entering Q_2+Z^2 is the area of Q_2, which is proportional to ϵ^2, the constant of proportionality depending only on A. Hence for some ω in P, this will be true and the inequality in (a) holds for this point for every sufficiently large N. But if it is true for ω and a fixed N, it is also true for some neighborhood P_a of ω for that N.

For the proof of (b), let l_2+v_0 be a translate of l_2 by a vector v_0 in Z^2 which intersects P. For some positive integer m_0, the parallelogram $T^{-m_0}Q,$ $+v_0$ will intersect P, thereby dividing P into 3 parallelograms, since T^mQ_1 tends to l_2 as $m\to\infty$. Let P_1 denote $P\cap(T^{-m_0}Q_1+v_0)$. Then $T^{m_0}(P_1)\subset Q_1+Z^2$. Consider an oriented parallelogram with center at v_0 whose width is $\frac{1}{2}$ the width of $T^{-m_0}Q_1+v_0$ and whose length is the length of $T^{-m_0}Q_1+v$ multiplied by $8\gamma^{-1}\epsilon^{-2}$ where γ is the sine of the angle between l_1 and l_2. $\gamma\epsilon^2$ is the area of Q_1, and thus the area of the resulting paralelogram is 4. It follows by the Minkowski theorem on convex bodies, that this parallelogram contains a lattice point v_0. Then it can be seen that $T^{-m_1}Q_1+v_1$

will intersect P_1, dividing it into 3 parts, provided that $|\lambda|^{m_1-m_0} \geqq 16\gamma^{-1}\epsilon^{-2}$. We may therefore take

$$m_1 = m_0 + [(\log|\lambda|)^{-1}\epsilon^{-2}] + 1 \leqq m_0 + \beta_2' + \beta_3' \log \epsilon^{-1}$$

where β_2' and β_3' depend only on A. We denote the intersection of $T^{-m_1}Q_1 + v_1$ and P_1 by P_2. Then $T^{m_0}(P_2) \subset Q_1 + Z^2$, $T^{m_1}(P_2) \subset Q_1 + Z^2$. In a similar manner we can find a lattice point v_2 in a parallelogram related to $T^{-m_1}Q_1 + v_1$ in the same way that the foregoing parallelogram of area 4 was related to $T^{-m_0}Q_1 + v_0$. For this v_2 we will have $T^{-m_2}Q_1 + v_2$ cutting P_2 into 3 portions, where $m_2 \leqq m_1 + \beta_2' + \beta_3 \log \epsilon^{-1}$. The intersection P_3 will satisfy $T^{m_i}(P_3) \subset Q_1 + Z^2$ for $i = 0, 1, 2$. Continuing in this way, we obtain parallelograms P_n with $T^{m_i}(P_n) \subset Q_1 + Z^2$ for $i = 0, 1, \cdots, n-1$, and with the integers $m_0, m_1, \cdots, m_{n-1}$ separated by a distance not exceeding $\beta_2' + \beta_3' \log \epsilon^{-1}$. Now take $\beta_2 = 2\beta_2'$, $\beta_3 = 2\beta_3'$, and $N = 2m$. The parallelogram P_b is then chosen as the P_n for $m_{n-1} < N \leqq m_n$. For then, the number of times $T^k P_b$ enter $Q_1 + Z^2$ exceeds n, and since $N \leqq m_n < m_0 + n(\beta_2' + \beta_3' \log \epsilon^{-1}) < N/2 + n/2(\beta_2 + \beta_3 \log \epsilon^{-1})$, we have

$$n > (\beta_2 + \beta_3 \log \epsilon^{-1})^{-1} N.$$

Now suppose ϵ to have been chosen so small that

$$\beta_1 \epsilon^2 < (\beta_2 + \beta_3 \log \epsilon^{-1})^{-1}.$$

Let P be an arbitrary oriented parallelogram in the plane and form the parallelograms P_a, $P_{ab} = (P_a)_b$, $P_{abc} = (P_{ab})_c$, etc., for a sequence of $N \to \infty$. Take ω as any point in the intersection of all the $P_{ab\cdots ab}$. Since ω belongs to infinitely many $P_{ab\cdots ab}$,

$$\limsup_{N\to\infty} N^{-1}\{\# \text{ of } T^n\omega,\ 0 \leqq n < N, \text{ such that } T^n\omega \in Q_1 + Z^2\} \geqq (\beta_2 + \beta_3 \log \epsilon^{-1})^{-1}.$$

On the other hand since ω belongs to infinitely many $P_{ab\cdots ba}$,

$$\liminf_{N\to\infty} N^{-1}\{\# \text{ of } T^n\omega,\ 0 \leqq n < N, \text{ with } T^n\omega \in Q_2 + Z^2\} \leqq \beta_1 \epsilon^2.$$

This ω has the desired properties and this proves the theorem.

COROLLARY. *If* λ *satisfies* $\lambda^2 - a\lambda + 1 = 0$ *where* a *is an integer, and* $|\lambda| > 1$, *then there exists a real number* t *such that* $\lim N^{-1} \sum_{n=0}^{N-1} e^{2\pi i \lambda^n t}$ *does not exist.*

Proof. Let $A = \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$; A has eigenvalues λ and λ^{-1}. Let e_1 and e_2

be two associated eigenvectors in R^2, $e_1 = \begin{pmatrix} e_1' \\ e_1'' \end{pmatrix}$, $e_2 = \begin{pmatrix} e_2' \\ e_2'' \end{pmatrix}$. Now let $u = xe_1 + ye_2$ be any vector in R^2. $T^n u = \lambda^n x e_1 + \lambda^{-n} y e_2$. The ergodic averages of $f(T^n u)$ will exist for any continuous doubly periodic function f if they exist for $f(u) = e^{2\pi i(ku' + lu'')}$ where $u = \begin{pmatrix} u' \\ u'' \end{pmatrix}$. Since $\lambda^{-n} \to 0$ it follows that the ergodic averages exist for all f if $\lim N^{-1} \sum_{n=0}^{N-1} e^{2\pi i \lambda^n (kxe_1' + lxe_1'')}$ exists for k, l, and x. By the foregoing theorem this is not the case and hence with $t = kxe_1' + lxe_1''$ for and appropriate choice of k, l, x, $\lim N^{-1} \sum e^{2\pi i \lambda^n t}$ will not exist.

In fact, the conclusion of this corollary requires only the hypothesis that $|\lambda| > 1$. This was pointed out to the author by Helson who has a very elegant proof of this result.

4. Extensions of strictly ergodic processes.

4.1. In § 2 we studied processes that were defined inductively from lower dimensional processes in the following manner: To each point ω_0 of a process (Ω_0, T_0, μ) we associate the circle $\omega_0 \times K$, and Ω is taken as the union of these circles. A tranformation T is defined on Ω by allowing T to permute the circles $\omega_0 \times K$ among themselves in accordance with T_0, and each circle is rotated by an amount depending on ω_0. In this section, we consider the more general situation where the transformation T on the individual circles is not necessarily a rotation, but any homeomorphism of the circle.

Definition 4. A process (Ω, T, μ) *extends* a process (Ω_0, T_0, μ_0) (and (Ω_0, T_0, μ_0) is a *subprocess* of (Ω, T, μ)), if there is a continuous map Φ taking Ω onto Ω_0 with $\Phi T = T_0 \Phi$ and with $\mu_0 = \Phi(\mu)$ in the sense that for any borel set Δ in Ω_0, $\mu_0(\Delta) = \mu(\Phi^{-1}(\Delta))$.

We notice that any subprocess of (Ω, T, μ) determines a subalgebra of $C(\Omega)$ by taking the set of functions $f = g \circ \Phi$. This subalgebra is isomorphic to $C(\Omega_0)$ and T_0 on $C(\Omega_0)$ is induced by T on $C(\Omega)$. Conversely one may show that any closed subalgebra of $C(\Omega)$, invariant under T, determines a subprocess. For example, the process $(K^r, T^{(r)}, m^r)$ defined by (2) in § 2 is an extension of $(K^s, T^{(s)}, m^s)$ for $s < r$ defined by restricting (2) to the first s coordinates $(\zeta_1, \cdots, \zeta_s)$. The subprocess thus corresponds to the subalgebras of functions on K^r depending only on $(\zeta_1, \cdots, \zeta_s)$. This subalgebra is invariant under T because each $T\zeta_i$ is a function of $\zeta_1, \cdots, \zeta_i$.

Definition 5. An extension (Ω, T, μ) of (Ω_0, T_0, μ_0) is *finite* if there is an integer $h > 0$ and a subset Λ of Ω of measure 0, such that almost every point $\omega_0 \in \Omega_0$ has at most h preimages in $\Omega - \Lambda$.

If $h = 1$, then (Ω, T, μ) is what has been called in [2] and L-extension of (Ω_0, T_0, μ_0). This means that the continuous functions on the extension Ω may be identified with measurable functions on Ω_0. Conversely under these circumstances h can be taken as 1.

The transformation T of K^2 given by $T\zeta_1 = e^{2\pi i\alpha}\zeta_1$, $T\zeta_2 = e^{2\pi i\alpha/h}\zeta_2$ leaves invariant a cycle on K^2. Consequently T defines a finite extension of (K, S_α, m) where $S_\alpha\zeta = e^{2\pi i\alpha}\zeta$.

The following theorem can be regarded as a generalization of Theorem 1. 3.

THEOREM 4. 1. *Let* (Ω_0, T_0, μ_0) *be a strictly ergodic process, let* $\Omega = \Omega_0 \times K$, *and let* T *be any continuous transformaton of* Ω *of the form* $T(\omega_0, \zeta) = (T_0\omega_0, g(\omega_0, \zeta))$ *where* $g: \Omega \rightarrow K$. *Then either* T *is a strictly ergodic transformation of* Ω *or there exists an invariant measure* μ *such that* (Ω, T, μ) *is a finite extension of* (Ω_0, T_0, μ_0). *Moreover, in the latter case, every invariant measure* μ *defines a finite extension.*

Remarks. If we define $\Phi: \Omega \rightarrow \Omega_0$ by $\Phi(\omega_0, \zeta) = \omega_0$, then the condition on T is just that T should extend T_0, i. e., that $\Phi T = T_0\Phi$. Since $\Phi(\mu)$ will therefore be invariant under T_0 if μ is invariant under T, and since μ_0 is the unique invariant measure for T_0, it follows that under these conditions (Ω, T, μ) necessarily extends (Ω_0, T_0, μ_0). We remark that Theorem 1. 3 is obtained from this theorem by taking for (Ω_0, T_0, μ_0) the trivial process for which Ω_0 consists of a single point.

Proof. Let M be the compact space of probability measures on K. An element of M is determined by a positive functional on $C(K)$ taking the value 1 at 1. We shall need the following observation. If H is a dense subset of $R(K)$, the set of real valued continuous functions on K, such that H is closed under additions, multiplication by rationals, and the lattice operations $\min(f, g)$, $\max(f, g)$, and $f \equiv 1 \in H$, then any functional on H which is linear over the rationals, which takes non-negative values for non-negative functions in H, and which takes the value 1 for the function 1 determines a unique measure in M. The reason is that any such functional can be extended to a linear, positive functional on $C(K)$, as one may easily show. The significance of this is due to the fact that H may be taken to be an enumerable subset of $C(K)$, and thus an enumerable number of conditions are imposed on a functional in order that it correspond to a measure in M.

Now consider the subsets of $\Omega = \Omega_0 \times K$ of the form $\Delta \times K$ with Δ a borel subset of Ω_0. These form a subfield B_0 of the borel field of Ω, and so we may speak of conditional expectations with respect to B_0. By the foregoing remarks it will follow that there exists an M-valued function on Ω_0, $\mu(\omega_0)$, such that these conditional expectations are obtained by

$$E(f|B_0)(\omega_0) = \int_K f(\omega_0,\zeta)\,d\mu(\omega_0)(\zeta) \tag{8}$$

for any bounded borel measurable function f on Ω. To construct $\mu(\omega_0)$ we apply (8) to functions $f(\omega_0,\zeta)=g(\zeta)$ where $g\in H$. The left hand side is defined almost everywhere and this defines a functional on H a.e. The fact that the functional may be defined on all of H a.e., is a consequence of the countability of H. Moreover from (8) if follows that at almost all ω_0, the functional obeys the enumerable set of conditions imposed in the preceding paragraph. Thus $\mu(\omega_0)$ is defined and it may be seen to be a measurable function from Ω_0 to M with the borel field on M induced by the weak topology on M (i.e. the topology for which M is compact: $\mu_n\to\mu$ if $\mu_n(f)\to\mu(f)$ for $f\in C(K)$). It follows that (8) is valid for f depending only on ζ, and from this, (8) follows for $f(\omega_0,\zeta)$ of the form $f_1(\omega_0)f_2(\zeta)$. It is clear then that (8) hold a.e. for any bounded borel measurable function on Ω.

From (8) and $E(E(f|B_0))=E(f)$ we obtain

$$\int_{\Omega_0}\{\int_K f(\omega_0,\zeta)\,d\mu(\omega_0)(\zeta)\}\,d\mu(\omega)=\int_\Omega f(\omega)\,d\mu(\omega). \tag{9}$$

We note also that (9) in turn uniquely determines the measurable function $\mu(\omega_0)$ up to sets of μ_0 measure 0, as can be seen by taking $f(\omega_0,\zeta)=f_1(\omega_0)f_2(\zeta)$.

Let $\{\zeta_1,\zeta_2\}$ denote, as in Theorem 1.3, the open arc on K from ζ_1 to ζ_2, taken counterclockwise. Let us define an M-valued function $\mu'(\omega_0)$ by

$$\mu'(\omega_0)(\{\zeta_1,\zeta_2\})=\mu(T\omega_0)(\{g(\omega_0,\zeta_1),g(\omega_0,\zeta_2)\})$$

where $T(\omega_0,\zeta)=(T_0\omega_0,g(\omega_0,\zeta))$. We then have

$$\begin{aligned}
&\int_{\Omega_0}\{\int_K f(\omega_0,\zeta)\,d\mu'(\omega_0)(\zeta)\}\,d\mu_0(\omega_0)\\
&\quad=\int_{\Omega_0}T_0\{\int_K f(T^{-1}(\omega_0,\zeta))\,d\mu(\omega_0)(\zeta)\}\,d\mu_0(\omega_0)\\
&\quad=\int_{\Omega_0}\{\int_K f(T^{-1}(\omega_0,\zeta))\,d\mu(\omega_0)(\zeta)\}\,d\mu_0(\omega_0)=\int_\Omega f(T^{-1}\omega)\,d\mu(\omega)\\
&\quad=\int_\Omega\{\int_{\Omega_0} f(\omega)\,d\mu(\omega)=\int_K f(\omega_0,\zeta)\,d\mu(\omega_0)(\zeta)\}\,d\mu_0(\omega_0).
\end{aligned}$$

But then $\mu'(\omega_0)=\mu(\omega_0)$ a.e. so that we have:

$$\mu(\omega_0)(\{\zeta_1,\zeta_2\})=\mu(T_0\omega_0)(\{g(\omega_0,\zeta_1),g(\omega_0,\zeta_2)\}) \tag{10}$$

almost everywhere. This says that T carries the associated measure $\mu(\omega_0)$ on $\omega_0 \times K$ onto the associated measure $\mu(T_0\omega_0)$ on $T_0\omega_0 \times K$. We shall refer to the $\mu(\omega_0)$ as the *relative* measures.

The condition that (Ω, T, μ) be a finite extension of (Ω_0, T_0, μ_0) may now be restated as the condition that for some h, the relative measures, $\mu(\omega_0)$, have their support, for almost all ω_0, on finite subsets of K having no more than h points. If, on the one hand, (Ω, T, μ) is a finite extension of (Ω_0, T_0, μ_0), then the measure $\mu'(\omega_0)$ obtained by restricting $\mu(\omega_0)$ to the points of K corresponding to $(\omega_0 \times K) \cap (\Omega - \Lambda)$, must agree a.e. with $\mu(\omega_0)$ since $\mu(\Lambda) = 0$. Hence $\mu(\omega_0)$ has its support a.e. on a set of $\leqq h$ points. Conversely suppose that $\mu(\omega_0)$ has its support a.e. on $\leqq h$ points. Define Λ as the union of the points (ω_0, ζ) for which ζ is not in the support of $\mu(\omega_0)$. We claim that Λ is a measurable set in Ω. To see this, take Γ_ϵ a compact set in Ω_0, with $\mu_0(\Gamma_\epsilon) > 1 - \epsilon$, $\epsilon > 0$, such that $\mu(\omega_0)$ is a continuous function from Γ_ϵ to M. This is possible because of the measurability of $\mu(\omega_0)$. On Γ_ϵ, the support of $\mu(\omega_0)$ is a continuous function (with range, the set of unordered h-tuples of points of K). Hence $\Lambda \cap \Gamma_\epsilon \times K$ is an open set and therefore measurable. But $\Lambda - \Lambda \cap \Gamma_\epsilon \times K$ has measure $\leqq \epsilon$ so that Λ is measurable. This type of argument may be used to verify a number of measurability assertions that we shall make. Now Λ must also have measure 0, by applying (9) to the indicator function of Λ. But $(\omega_0 \times K) \cap (\Omega - \Lambda)$ has $\leqq h$ points for every ω_0, and so $\Phi^{-1}(\omega_0) \cap (\Omega - \Lambda)$ has $\leqq h$ points so that (Ω, T, μ) is a finite extension of (Ω_0, T_0, μ). It should be pointed out that the set of points (ω_0, ζ) with ζ in the support of $\mu(\omega_0)$ may be much smaller than the support of μ. Thus if each $\mu(\omega_0)$ is concentrated at one point $\zeta = \phi(\omega_0)$, the support of μ will be the closure of $\{(\omega_0, \phi(\omega_0))\}$ which may be all of Ω.

Now suppose that μ is an ergodic invariant measure for T, that does not define a finite extension of (Ω_0, T_0, μ_0); then a.e., $\mu(\omega_0)$ has infinite support. We claim that in this case, $\mu(\omega_0)$ is, a.e., a non-atomic measure, i.e. it has no discrete component. Otherwise define $\Delta_\delta(\omega_0) = \{(\omega_0, \zeta) : \mu(\omega_0)(\{\zeta\}) > \delta\}$ for $\delta > 0$, and let $\Delta_\delta = \bigcup_{\omega_0 \in \Omega_0} \Delta_\delta(\omega_0)$. Again one can show that Δ_δ is measurable by considering $\Delta_\delta \cap (\Gamma \times K)$ where Γ is compact and $\mu(\omega_0)$ is continuous when restricted to Γ. Now (10) shows that Δ_δ is invariant under T; hence Δ_δ has either measure 0 or 1. This in turn implies that almost all $\Delta_\delta(\omega_0)$ have measure 0 or 1. The latter would imply that $\mu(\omega_0)$ has its support on $\leqq \delta^{-1}$ points of K contrary to our assumption. Hence $\Delta_\delta(\omega_0)$ has measure 0 with probability 1, which implies that $\Delta_\delta(\omega_0)$ is a.e. empty. Letting $\delta \to 0$ shows that $\mu(\omega_0)$ is a.e. non-atomic.

Under the assumption that an ergodic, invariant μ exists that does not define a finite extension, one can show that no other invariant measure ν on (Ω, T) can define a finite extension. For suppose that ν is an ergodic measure with $\nu(\omega_0)$ having its support on $\leqq h$ points for almost all ω_0. The unordered h-tuple $\{\zeta_1(\omega_0), \cdots, \zeta_h(\omega_0)\}$ on which $\nu(\omega_0)$ has its support is a measurable function of ω_0. Note that h is independent of ω_0, since the set of ω_0 having h points in the support of $\mu(\omega_0)$ is invariant under T_0 by (10). Now consider for each ω_0, the set of points

$$\Delta(\omega_0) = \{\zeta \in K : \mu(\omega_0)(\{\zeta_i(\omega_0), \zeta\}) \leqq \epsilon \text{ for some } i = 1, \cdots, h\},$$

and take $\Delta = \bigcup_{\omega_0 \in \Omega_0} (\omega_0 \times \Delta(\omega))$. Again Δ is a measurable subset of Ω, and by (10), Δ is invariant under T. But by (9), $\epsilon \leqq \mu(\Delta) \leqq h\epsilon$ contrary to the assumption that μ is ergodic, if $0 < \epsilon < h^{-1}$. This shows that if an ergodic infinite extension exists, every extension is infinite.

Now suppose that μ and μ' are two invariant measures on (Ω, T), with $\mu(\omega_0)$ and $\mu'(\omega_0)$ non-atomic a.e. Let $\lambda = \frac{1}{2}(\mu + \mu')$ so that $\lambda(\omega_0)$ is again non-atomic a.e. Fix a point $\zeta_0 \in K$ and consider the map Ψ from $\Omega = \Omega_0 \times K \rightarrow \Omega' = \Omega_0 \times K'$ (K' is the unit circle in the complex plane) given by

$$\Psi(\omega_0, \zeta) = (\omega_0, e^{2\pi i \lambda(\omega_0)(\{\zeta_0, \zeta\})}). \tag{11}$$

As in the proof of Theorem 1.3, we have that if $\zeta_1, \zeta_2, \zeta_3 \in K$,

$$\lambda(\omega_0)(\{\zeta_1, \zeta_2\}) + \lambda(\omega_0)(\{\zeta_2, \zeta_3\}) \equiv \lambda(\omega_0)(\{\zeta_1, \zeta_3\}) \pmod 1.$$

Hence we have

$$\begin{aligned} \Psi(T(\omega_0, \zeta)) &= (T_0\omega_0, e^{2\pi i \lambda(T_0\omega_0)(\{\zeta_0, g(\omega_0, \zeta)\})}) \\ &= (T_0\omega_0, e^{2\pi i \lambda(T_0\omega_0)(\{\zeta_0, g(\omega_0, \zeta_0)\})}\, e^{2\pi i \lambda(T_0\omega_0)(\{g(\omega_0, \zeta_0), g(\omega_0, \zeta)\})}) \\ &= (T_0\omega_0, g(\omega_0)\, e^{2\pi i \lambda(\omega_0)(\{\zeta_0, \zeta\})}) \end{aligned}$$

where $g(\omega_0) = e^{2\pi i \lambda(T_0\omega_0)(\{\zeta_0, g(\omega_0, \zeta_0)\})}$, the last equality being a consequence of (10). Hence, taking $S(\omega_0, \zeta) = (T_0\omega_0, g(\omega_0)\zeta)$, we have

$$\Psi T(\omega_0, \zeta) = S\Psi(\omega_0, \zeta). \tag{12}$$

Here it can be shown that the mappings Ψ and S are measurable. In fact, on a compact set Γ relative to which $\lambda(\omega_0)$ and $\lambda(T_0\omega_0)$ are continuous, the functions $\lambda(\omega_0)(\{\zeta_0, \zeta\})$ and $\lambda(T_0\omega_0)(\{\zeta_0, g(\omega_0, \zeta_0)\})$, entering in the definition of Ψ and S, are actually continuous. This is so because $\lambda(\omega_0)$ is non-atomic.

It is clear from (9) and (11) that Ψ takes the measure λ on Ω into the product measure $\mu_0 \times m$ on Ω', in the sense that $\mu_0 \times m(\Delta) = \lambda(\Psi^{-1}(\Delta))$, or, equivalently, that $\lambda(f\circ\Psi)=\mu_0\times m(f)$. We write $\Psi(\lambda)=\mu_0\times m$. Let μ_* and μ_*' denote respectively $\Psi(\mu)$ and $\Psi(\mu')$, i.e. the images of μ and μ' under the map Ψ. We have then $\mu_0\times m=\frac{1}{2}(\mu_*+\mu_*')$. But $T\mu=\mu$ implies $\Psi(T\mu)=\Psi(\mu)$ so that by (12), $S(\Psi(\mu))=\Psi(\mu)$, or $S\mu_*=\mu_*$. Similarly $S\mu_*'=\mu_*'$. Thus S is not an ergodic transformation for $\mu\times m$ unless $\mu_*=\mu_*'$.

Assuming $\mu_*\neq\mu_*'$ it follows that S is not ergodic. The Fourier series argument of Lemma 2.1 applies as well here (for $g(\omega_0)$ measurable rather than continuous), and we deduce that for some $k\neq 0$,

$$g^k(\omega_0)=R(T_0\omega_0)/R(\omega_0).$$

For every interval $\Delta\subset K'$, we may define

$$\Lambda'(\Delta)=\{(\omega_0,\zeta)\in\Omega':R(\omega_0)^{-1}\zeta^k\in\Delta\}.$$

It is readily verified that $\mu_0\times m(\Lambda'(\Delta))=m(\Delta)$. Now $\Lambda'(\Delta)$ is invariant under S, since if $R(\omega_0)^{-1}\zeta^k\in\Delta$ then $R(T_0\omega_0)^{-1}g_0{}^k(\omega_0)\zeta^k\in\Delta$ which is just the condition for $S(\omega_0,\zeta)\in\Lambda'(\Delta)$. Since $m(\Delta)$ is arbitrary, it follows that S has invariant sets of all measures between 0 and 1. From (12) it follows that if $\Lambda'(\Delta)$ is invariant under S, then $\Lambda(\Delta)=\Psi^{-1}(\Lambda'(\Delta))$ is invariant under T. Since Ψ takes λ into $\mu_0\times m$ it follows that there are invariant sets on Ω of arbitrary λ-measure. But we assumed that μ and μ' were ergodic measures and $\lambda=\frac{1}{2}(\mu+\mu')$. If a measurable set is invariant under T, it must have μ-measure 0 or 1 and μ'-measure 0 or 1. Hence it must have λ-measure 0, $\frac{1}{2}$, or 1. Thus we are led to a contradiction which means that $\mu_*=\mu_*'$.

From this we shall deduce that $\mu=\mu'$. For this it suffices to show that $\mu(\omega_0)=\mu'(\omega_0)$ a.e. But clearly the relative measures of μ and μ' are mapped into the relative measures of μ_* and μ_*' by Ψ. Since $\mu_*=\mu_*'$, we have $\mu_*(\omega_0)=\mu_*'(\omega_0)$ a.e. To complete the proof it suffices to show that the relative measure $\mu(\omega_0)$ is determined a.e. by its image $\mu_*(\omega_0)$ and similarly for μ'. Here we are considering the relative measure $\mu(\omega_0)$ on $\omega_0\times K$, and by its image we mean the image under Ψ on $\omega_0\times K'$. Now $\mu(\omega_0)$ and $\mu'(\omega_0)$ are both absolutely continuous with respect to $\lambda(\omega_0)$ which is carried onto lebesgue measure on $\omega_0\times K'$. If an interval and a subinterval of $\omega_0\times K$ both map onto the some interval af $\omega_0\times K'$ under Ψ, the $\lambda(\omega_0)$-measure of the difference must be 0, by (11), and a foriori the $\mu(\omega_0)$- and $\mu'(\omega_0)$-measures will be 0. It follows that the $\mu(\omega_0)$-measure of any interval of $\omega_0\times K$ is the same as that of the preimage of the image of the interval under Ψ, and hence the same as the $\mu_*(\omega_0)$-measure of its image under Ψ. Consequently $\mu(\omega_0)$ is determined by $\mu_*(\omega_0)$ and similarly for $\mu'(\omega_0)$. Therefore $\mu = \mu'$.

This completes the proof of the theorem. For we have shown that if there exists some infinite ergodic extension (Ω, T, μ) of (Ω_0, T_0, μ_0) then no ergodic extensions can be finite. In addition we have just shown that any other ergodic extension must be identical with the first. Thus unless T is strictly ergodic, all ergodic extensions must be finite.

The simplest example of this theorem for dimension > 1 is for $\Omega = K^2$ and $T\zeta_1 = e^{2\pi i\alpha}\zeta_1$, $T\zeta_2 = g(\zeta_1, \zeta_2)$. Our theorem asserts that there are two alternatives. Either T is strictly ergodic or all invariant measures on K^2 define finite extensions of (K, S_α, m), where $S_\alpha\zeta = e^{2\pi i\alpha}\zeta$. The latter alternative implies in particular that for some $h > 0$ there exists a measurable function $\Delta(\zeta_1)$ with its range in the space of unordered h-tuples of points on K, and with $\Delta(e^{2\pi i\alpha}\zeta) = g(\zeta, \Delta(\zeta)) = \{g(\zeta, \zeta') : \zeta' \in \Delta(\zeta)\}$. In particular for $h = 1$, this would mean the existence of a solution to $R(e^{2\pi i\alpha}\zeta) = g(\zeta, R(\zeta))$. The set $\Delta(\zeta)$ is here simply the support of the relative measure $\mu(\zeta)$ defined by the extension. Needless to say, in practice it is difficult to ascertain which of the two alternatives actually occurs. Theorem 2.1 gives the only cases for which we have resolved this question.[1]

5. A fixed point theorem and existence of an almost periodic subprocess.

5.1. We restrict our attention once again to the two-dimensional torus K^2. In the last section we saw that if the transformation T on K^2 has a certain form then some assertions could be made regarding the strict ergodicity of T. We now inquire when a general transformation T of K^2 can, by an appropriate choice of coordinates, be put into the specified form. We are not able to fully answer this question; however we can give conditions on T under which it will almost have the required form. To be precise, the condition on T in the last section was that it define an extension of a 1-dimensional process (K, S_α, m), and that one of the two coordinate functions on K^2 can be taken for the coordinate function on K. What we shall obtain are sufficient conditions for the existence of a subprocess (K, S_α, m) for (K^2, T, μ), but the coordinate function for K may not be a possible coordinate function for K^2. The reason is that a function from K^2 to K will be a coordinate function for

---

[1] *Added in proof*: There is a corollary to the proof of this theorem which is worth noting. In case $T\zeta_1 = e^{2\pi i\alpha}\zeta_1$, $T\zeta_2 = g(\zeta_1, \zeta_2)$ does not define a finite extension of (K, S_α, m), then eq. (12) establishes a measure theoretic isomorphism between the process in question and the "standard" process of eq. (2) ($r = 2$) in § 2.1.

K^2 only if its level sets are homeomorphic to a circle, and this need not happen for the mapping function from K^2 to K in our case.

If a process (K^2, T, μ) extend some (K, S_α, m) then by Definition 4, the associated map $\phi\colon K^2 \to K$ satisfies $\phi T = S_\alpha \phi$. Looking at ϕ as a function in $C(K^2)$, ϕT is the function we have denoted $T\phi$. Moreover, $S_\alpha \phi = e^{2\pi i\alpha}\phi$, so that (K^2, T, μ) extends (K, S_α, m) only if there exists a solution to $T\phi = e^{2\pi i\alpha}\phi$, i.e. a non-constant eigenfunction of T, in $C(K^2)$. Conversely if there exists such an eigenfunction ϕ, then the algebra of functions of ϕ is invariant under T and so determines a subprocess which will be isomorphic to (K, S_α, m). The main result of this section is the following:

THEOREM 5.1. *If T is a homeomorphism of K^2 leaving no proper closed subset of K^2 invariant and if T is not homotopic to the identity transformation then there exists a continuous eigenfunction $\phi\colon T\phi = e^{2\pi i\alpha}\phi$ where α is irrational.*

For the proof of this we shall require two preliminary results, the first of which is a fixed point theorem which is of some independent interest.

LEMMA 5.1. *Let $S\colon K^2 \to K^2$ be a homeomorphism of the form $S\zeta_1 = \zeta_1 e^{2\pi i G(\zeta_1,\zeta_2)}$, $S\zeta_2 = \zeta_1^d \zeta_2 e^{2\pi i H(\zeta_1,\zeta_2)}$ where G and H are continuous real valued functions on K^2. Then if $d \neq 0$ and $\sup_{\omega',\omega'' \in K^2} | G(\omega') - G(\omega'') | \geqq 7$, then the transformation S must have a fixed point.*

Remark. The form of S as given here is the most general one for which S is homotopic to the linear map $\bar{S}\zeta_1 = \zeta_1$, $\bar{S}\zeta_2 = \zeta_1^d \zeta_2$. We know from § 3 that up to a change of coordinates, this is the most general form which S can have if it is not to have a fixed point by virtue of the Lefshetz fixed point theorem. The present lemma gives conditions under which a fixed point must exist even if the homotopy class of S does not require the existence of a fixed point.

Proof. Let ρ_1 denote the cycle $\{\lambda_2 = 1\}$ and ρ_2, the cycle $\{\zeta_1 = 1\}$. By a cycle we shall always mean a continuous 1-1 image of K. To prove that there is a fixed point we shall show that for every $\epsilon > 0$ there are points $\omega \in K^2$ with $| S\zeta_1(\omega) - \zeta_1(\omega) | < \epsilon$ and $| S\zeta_2(\omega) - \zeta_2(\omega) | < \epsilon$ simultaneously. By compactness there will have to be a fixed point.

Let $\Gamma = \{\omega : | S\zeta_2(\omega) - \zeta_2(\omega) | < \epsilon\} = \{\omega : | \zeta_1^d e^{2\pi i H(\zeta_1,\zeta_2)} - 1 | < \epsilon\}$. On $K^2 - \Gamma$, the function $\zeta_1^d e^{2\pi i H(\zeta_1,\zeta_2)}$ does not take on the value 1. Hence it is an inessential map and the function ζ_1^d which is homotopic to it is also inessential. Since $d \neq 0$ it follows that ζ_1 is also inessential on $K^2 - \Gamma$. Consequently on any cycle in Γ close to the boundary of Γ, ζ_1 is inessential. There are now two cases to consider. Suppose first that there is some homologically non-trival (relative to K^2) cycle in Γ arbitrarily close to the boundary of Γ. Since ζ_1 is inessential on this cycle, the cycle must be homologous to a multiple of ρ_2. But a cycle homologous to $l\rho_2$ with $|l| > 1$, contains a cycle homologous to ρ_2, so that there is in Γ a cycle homologous to ρ_2. If, on the other hand, all cycles in Γ sufficiently close to the boundary of Γ are homologous to 0 in K^2, it is easily seen that Γ contains a cycle in every homology class and in particular one homologous to ρ_2. Thus, in either case, Γ contains a cycle γ homologous to ρ_2.

To show that there is a point ω in K^2 with $|S\zeta_1(\omega) - \zeta_1(\omega)| < \epsilon$, $|S\zeta_2(\omega) - \zeta_2(\omega)| < \epsilon$, it suffices to show that $|e^{2\pi i G(\omega)} - 1|$ becomes $< \epsilon$ on γ. For this it suffices to show that for arbitrarily small $\delta > 0$, $G(\omega)$ oscillates on γ by an amount $> 1 - \delta$. Now suppose that on γ, $G(\omega)$ oscillates by $\leqq 1 - \delta$ for some $\delta > 0$. Let $[a, b]$ be the range of $G(\omega)$ on K^2, so that $b - a \geqq 7$, and let $[a', b'] \subset [a, b]$ be the range of $G(\omega)$ on γ, so that $b' - a' \leqq 1 - \delta$. One of the intervals (a, a') or (b', b) has length $\geqq 3 + \delta/2$. Assume it is the first, the argument being entirely analogous if it is the second, so that $a' - a \geqq 3 + \delta/2$. Let Δ be the set of points on K^2 for which $G(\omega)$ lies in (a, a'). We shall show that Δ contains a cycle homologous to ρ_1. Since any cycle homologous to ρ_1 intersects any cycle homologous to ρ_2 it will follow that γ must intersect Δ contrary to the supposition that on γ, $G(\omega)$ omits the values in (a, a'). This contradiction implies that $G(\omega)$ does oscillate by $> 1 - \delta$ on γ and the desired point ω exists.

We now lift the map S to a map S^* of the plane. If we assume that the point $(0, 0)$ in R^2 corresponds to $(1, 1)$ in K^2, then S will have the form

$$\begin{aligned} \theta_1^* &= S^*\theta_1 = \theta_1 + G(\theta_1, \theta_2) \\ \theta_2^* &= S^*\theta_2 = d\theta_1 + \theta_2 + H(\theta_1, \theta_2). \end{aligned} \tag{13}$$

Let Σ denote the strip in R^2 given by $0 \leqq \theta_1 \leqq 1$. Δ lifts to a set Δ^* in the plane on which $G(\theta_1, \theta_2)$ takes values in (a, a_1). Hence $\Delta^* \cap \Sigma$ contains at least those points for which $a + 1 \leqq \theta_1 + G(\theta_1, \theta_2) < a_1$, i.e., the points for which $a + 1 \leqq \theta_1^* < a_1$. To show that Δ contains a cycle homologous to ρ_1, we will prove that for some θ_2 there is a curve joining $(0, \theta_2)$ to $(1, \theta_2)$ in Σ for which $a + 1 < \theta_1^* < a_1$. Such a curve maps onto a cycle homologous to ρ_1 and lying in Δ.

The function θ_1^* is well defined on R^2 and hence if a point (θ_1, θ_2) belongs to the curve $\{\theta_1^* = C\}$, then the point $(\theta_1 + 1, \theta_2)$ cannot also belong to this curve since $\theta_1^*(\theta_1 + 1, \theta_2) = C + 1$ by (13). A less evident fact is that $(\theta_1 + t, \theta_2)$ cannot belong to $\{\theta_1^* = C\}$ if (θ_1, θ_2) does, for any $t \geqq 1$. To see this we note that if (θ_1, θ_2) and $(\theta_1 + t, \theta_2)$ belong to $\{\theta_1 = C\}$ for $t \geqq 1$, then since $\{\theta_1^* = C\}$ is connected (since S^* is a homeomorphism) it follows that for some $(\theta_1', \theta_2') \in \{\theta_1^* = C\}$, we will also have $(\theta_1' + 1, \theta_2') \in \{\theta_1^* = C\}$. From this we conclude that on a line segment: $\theta_2 = \theta_2'$, $\theta_1' \leqq \theta_1 \leqq \theta_1' + 1$, the function θ_1^* cannot takes values $\geqq \theta_1^*(\theta_1', \theta_2') + 2$ or $\leqq \theta_1^*(\theta_1, \theta_2') - 1$. For if at a point (θ_1, θ_2') in this segment $\theta_1^*(\theta_1, \theta_2') \geqq \theta_1^*(\theta_1', \theta_2') + 2$ then $\theta_1^*(\theta_1 - 1, \theta_2') \geqq \theta_1^*(\theta_1' + 1, \theta_2')$. But every value of θ_1^* exceeding $\theta_1^*(\theta_1' + 1, \theta_2')$ occurs at some $(\theta_1'', \theta_2'), \theta_1'' > \theta_1' + 1$ and $\theta_1'' - (\theta_1 - 1) \geqq 1$ since $\theta_1 \leqq \theta_1' + 1 \leqq \theta_1''$. A similar argument gives the other inequality.

Now in Σ, $G(\theta_1, \theta_2)$ attains its maximum and its minimum, so that θ_1^* must attain a maximum $\geqq b$ and a minimum $\leqq a + 1$ in Σ. Also if S^* is a homeomorphism, θ_1^* cannot attain its maximum in Σ at an interior point of Σ. This implies that on the line $\theta_1 = 0$, θ_1^* attains a minimum $\leqq a + 1$ and a maximum $\geqq b - 1$. In particular, θ_1^* will vary between $a + 1$ and $a + 2 + \delta/2 < b - 1$ on $\theta_1 = 0$. There will therefore be an interval $\theta_2^{(1)} \leqq \theta_2 \leqq \theta_2^{(2)}$ on $\theta_1 = 0$ on which θ_1^* varies from $a + 1 + \delta/4$ to $a + 2 + \delta/4$ as θ_2 goes from $\theta_3^{(1)}$ to $\theta_2^{(2)}$ and such that neither extreme value of θ_1^* occurs in the interior of this interval.

Let Λ^* be the relatively open set in Σ defined by the condition that $a + 1 < \theta_1^* < a + 3 + \delta/2$. $\Lambda^* \subset \Delta^* \cap \Sigma$ since $a + 3 + \delta/2 \leqq a_1$. The interval on $\theta_1 = 0$ from $(0, \theta_2^{(1)})$ to $(0, \theta_2^{(2)})$ lies in Λ^*; let Λ_0^* be the connected component of Λ^* containing this interval. We claim that the point $(1, \theta_2^{(2)})$, which belongs to Λ^* because

$$\theta_1^*(1, \theta_2^{(2)}) = 1 + \theta_1^*(0, \theta^{(2)}) = a + 3 + \delta/4 < a + 3 + \delta/2,$$

actually belongs to Λ_0^*. Suppose that this were not the case. Then one of the bounding lines $\theta_1^* = a + 1$ or $\theta_1^* = a + 3 + \delta/2$ must separate $(1, \theta_2^{(2)})$ from $(0, \theta_3^{(2)})$ and $(0, \theta_3^{(1)})$. But on the segment from $(0, \theta_2^{(2)})$ to $(1, \theta_2^{(2)})$, θ_1^* cannot take a value less than $a + 1 + \delta/4$, since $\theta_1^*(0, \theta_2^{(2)}) = a + 2 + \delta/4$. Hence the line $\theta_1^* = a + 1$ cannot separate the two points. On the other hand, the same reasoning shows that θ_1^* cannot exceed $a + 3 + \delta/4$ on the line segment joining $(0, \theta_2^{(1)})$ to $(1, \theta_2^{(1)})$. Hence the line $\theta_1^* = a + 3 + \delta/2$ separating $(1, \theta_2^{(2)})$ from Λ_0^* cannot pass below the level $\theta_2 = \theta_2^{(1)}$. In order to separate $(0, \theta_2^{(2)})$ from $(1, \theta_2^{(2)})$ it must however pass below the level $\theta_3 = \theta_2^{(2)}$. Hence on one of the lines $\theta_1 = 0$, 1, it lies between the levels $\theta_2 = \theta_2^{(1)}$ and $\theta_2^{(2)}$. This means that in the interval $\theta_2^{(1)} < \theta_2 < \theta_2^{(2)}$ on $\theta_1 = 0$, θ_1^* takes on either the value $a + 3 + \delta/2$ or $a + 2 + \delta/2$. Both of these are impossible since in the interior of the interval in question $\theta_1^* < a + 2 + \delta/4$.

This shows that $(1, \theta_2^{(2)}) \in \Delta_0^*$, so that there exists a curve β joining $(0, \theta_2^{(2)})$ to $(1, \theta_2^{(2)})$ lying wholly in $\Lambda^* \subset \Delta^*$. It follows that β maps onto a cycle in K^2 homologous to ρ_1 and lying in Δ. This completes the proof of the lemma.

LEMMA 5.2. *Let T be a transformation of a compact metric space Ω leaving no proper closed subset of Ω invariant. If $f \in C(\Omega)$, then a necessary and sufficient condition for $f = Tg - g$ with $g \in C(\Omega)$, is that the functions $f + Tf + \cdots + T^n f$ are uniformly bounded.*

This lemma appears in [3], p. 135 and, in slightly disguised form, in [2], p. 164.

5.2. *Proof of Theorem* 5.1. From the fact that T has no fixed point we may infer that T has the form of S in Lemma 5.1, for some choice of coordinates (ζ_1, ζ_2). In these coordinates

$$T^n \zeta_1 = \zeta_1 e^{2\pi i (G(T^{n-1}\omega) + \cdots + G(\omega))}$$
$$T^n \zeta_2 = \zeta_1^{nd} \zeta_2 e^{2\pi i H_n(\omega)}$$

for some continuous real valued function H_n, as may be seen by induction. Thus T^n also has the form of S, just with different values of d. Since no power of T has a fixed point if T leaves no proper closed subset of K^2 invariant, Lemma 5.1 implies that for every n, the function $(G(T^{n-1}\omega) + \cdots + G(\omega))$ oscillates by < 7 on K^2. Now for some ω, $\lim n^{-1}(G(T^{n-1}\omega) + \cdots + G(\omega)) = \alpha$ exists by the ergodic theorem applied to some stationary measure on K^2. It follows that this limit exists and equals α for all ω in K^2, and therefore for any invariant probability measure μ, $\mu(G) = \alpha$. Now take $G'(\omega) = G(\omega) - \alpha$; then $\mu(G'(T^{n-1}\omega) + \cdots + G'(\omega)) = 0$. It follows that in K^2, $G'(T^{n-1}\omega) + \cdots + G'(\omega)$ cannot be everywhere strictly positive or strictly negative. Since this expression oscillates by < 7 it follows that

$$| G'(T^{n-1}\omega) + \cdots + G'(\omega) | < 7$$

for all n. We may now apply Lemma 5.2 since T leaves no proper closed subset of K^2 invariant. We conclude that there exists a continuous function $Q(\omega)$ on K^2 with $G'(\omega) = Q(T\omega) - Q(\omega)$, whence $G(\omega) = Q(T\omega) - Q(\omega) + \alpha$. Hence $T\zeta_1 = \zeta_1 e^{2\pi i [Q(T\omega) - Q(\omega) + \alpha]}$ and $T(\zeta_1 e^{-2\pi i Q(\omega)}) = e^{2\pi i \alpha}(\zeta_1 e^{-2\pi i Q(\omega)})$ so that $\phi(\omega) = \zeta_1 e^{-2\pi i Q(\omega)}$ is the eigenfunction sought. Here α must be irrational since if $\alpha = l/k$, then the set of ω for which $\phi(\omega) = e^{2\pi i \nu/k}$, $\nu = 0, 1, \cdots, k-1$, would be a proper closed subset of K^2. (Since $\phi(\omega)$ is homotopic to ζ_1, it is an essential map and therefore $\phi(\omega)$ takes on all values on the unit circle.) This concludes the proof of the theorem.

REFERENCES.

[1] A. Denjoy, " Sur les courbes définies par les équations differentielles a la surface du tore," *Journal de Mathémathiques* (9) t. 11 (1932), pp. 333-375.

[2] H. Furstenberg, *Stationary Processes and Prediction Theory*, Princeton University Press, Princeton (1960).

[3] W. H. Gottschalk and G. A. Hedlund, *Topological Dynamics*, Amer. Math. Soc. Coll. Publ., Vol. 36, Providence (1955).

[4] E. W. Hobson, *The Theory of Functions of a Real Variable*, second edition, Vol. II, Harren Press, Washington, D. C. (1950).

[5] E. R. van Kampen, " The topological transformations of a simple closed curve," *American Journal of Mathematics*, vol. 57 (1935), pp. 142-152.

[6] N. Kryloff and N. Bogoliuboff, " La théorie générale de la mesure dans son application a l'étude des systemes dynamiques non linéaires," *Annals of Mathematics*, vol. 38 (1937), pp. 65-113.

[7] B. Lawton, "A note on well-distributed sequences," *Proceedings of the American Mathematical Society*, vol. 10, No. 6 (1959), pp. 891-892.

[8] V. V. Nemytzkii and V. V. Stepanov, *Qualitative Theory of Differential Equations*, Princeton University Press, Princeton (1960).

[9] J. C. Oxtoby, " Ergodic sets," *Bulletin of the American Mathematical Society*, vol. 58 (1952), pp. 116-136.

[10] G. M. Peterson, "Almost convergence and uniformly distributed sequences," *Quarterly Journal of Mathematics*, vol. 7 (1956), pp. 188-191.

[11] Antoni Zygmund, *Trigonometric Series*, second edition, University Press, Cambridge (1959).

ON THE SUMMABILITY, BY SPHERICAL RIESZ MEANS, OF DERIVED MULTIPLE FOURIER SERIES.*

By A. J. White.

---

1. **Introduction.** We suppose, throughout this paper that $f(x) \equiv f(x_1, \cdots, x_k)$ is integrable in the Lebesgue sense in $0 \leqq x_i \leqq 2\pi$ $(i = 1, \cdots, k)$ and is periodic, with period 2π in each variable. The Fourier series of $f(x)$ may be written

$$f(x) \sim \sum_{n_1 \cdots n_k = -\infty}^{\infty} \cdots \sum a_{n_1 \cdots n_k} e^{i(n_1 x_1 + \cdots + n_k x_k)},$$

where

$$a_{n_1 \cdots n_k} = (2\pi)^{-k} \int_{x_1 \cdots x_k = 0}^{2\pi} \cdots \int f(x) e^{-i(n_1 x_1 + \cdots + n_k x_k)} dx_1 \cdots dx_k.$$

We write[1]

$$A_n(x) = \sum_{n = n_1^2 + \cdots + n_k^2} a_{n_1 \cdots n_k} e^{i(n_1 x_1 + \cdots + n_k x_k)},$$

with the convention that $A_n(x) \equiv 0$ if n cannot be expressed as the sum of k squares of integers. We form $B_n(x)$ from the series

$$\sum_{n_1 \cdots n_k = -\infty}^{\infty} \cdots \sum b_{n_1 \cdots n_k} e^{i(n_1 x_1 + \cdots + n_k x_k)},$$

where the $b_{n_1 \cdots n_k}$ are arbitrary complex numbers, in a similar way.

The spherical mean, $f_{x^0}(t)$ of the function $f(x)$ at the point $x^0 \equiv (x_1^0, \cdots, x_k^0)$ is defined by

$$f_{x^0}(t) = \frac{\Gamma(\frac{1}{2}k)}{2(\pi)^{\frac{1}{2}k}} \int_\sigma f(x_1^0 + t\xi_1, \cdots, x_k^0 + t\xi_k) \, d\sigma_\xi \qquad (k \geqq 2)$$

where σ is the sphere $\xi_1^2 + \cdots + \xi_k^2 = 1$ and $d\sigma_\xi$ its $(k-1)$-dimensional volume element. If $k = 1$ then

$$f_{x^0}(t) = \tfrac{1}{2}\{f(x^0 + t) + f(x^0 - t)\}.$$

Riesz means $S_R^\delta(f, x)$, of order δ and type n, of the series $\sum_{n=0}^{\infty} A_n(x)$ are defined by

---

* Received March 30, 1961.

[1] The theory of spherical summability of multiple Fourier series was initiated by Bochner [2]. An introduction and an account of the main results is given in [7].

$$S_R^0(f,x) = S_R(f,x) = \sum_{n\leqq R^2} A_n(x)$$

$$S_R^\delta(f,x) = 2\delta/R^2 \int_0^R (1-u^2/R^2)^{\delta-1} u S_u(f,u)\,du \qquad (\delta > 0)$$

$$= \sum_{n\leqq R^2} (1-n/R^2)^\delta A_n(x). \qquad (\delta > 0)$$

The Laplacian $\Delta_x{}^q$, defined by

$$\Delta_x{}^1 = \frac{\partial^2}{\partial x_1{}^2} + \cdot\cdot\cdot + \frac{\partial^2}{\partial x_k{}^2}$$

$$\Delta_x{}^{r+1} = \Delta_x{}^1(\Delta_x{}^r) \qquad (r = 1, 2, \cdot\cdot\cdot)$$

applied to the terms of the series $\sum_{n=0}^{\infty} A_n(x)$ yields

$$(1.1) \qquad (-)^q \sum_{n=1}^{\infty} n^q A_n(x).$$

Observing that

$$\Delta_x{}^q S_R{}^\delta(f,x) = (-)^q \sum_{n\leqq R^2} (1-n/R^2)^\delta n^q A_n(x),$$

we may state known results concerning the summability, by Riesz means, of the series (1.1), in the following form.

THEOREM A.[2] *If there exists a polynomial $P(t)$, in t^2, of degree $2(q-1)$ $(\geqq 0)$ such that*

$$f_x(t) - P(t) \sim \frac{st^{2q}\Gamma(\frac{1}{2}k)}{2^{2q}q!\,\Gamma(q+\frac{1}{2}k)},$$

as $t \to +0$, then

$$\Delta_x{}^q S_R{}^\delta(f,x) \to s$$

as $R\to\infty$, whenever $\delta > 2q + \frac{1}{2}(k-1)$.

THEOREM B.[3] *Suppose that the trigonometric series $\sum_{n=0}^{\infty} B_n(x)$ is summable*[4] *(n,δ) to s, for a non-negative integer δ, and that, for some $\epsilon > 0$, $B_n(0) = o(n^{\delta-\epsilon})$. Then if q $(> \delta + 1)$ is a positive integer, and if*

$$g(x) = \frac{B_0(x_1 + \cdot\cdot\cdot + x_k)^{2q}}{k^q(2q)!} + (-)^q \sum_{n=1}^{\infty} n^{-q} B_n(x),$$

---

[2] Theorems A and B are given by Shapiro ([9] Theorems 2, 3 and 5). We have altered his notation slightly.

[3] Shapiro has obtained a sharper version of this Theorem (see [10] Theorem 2).

[4] I. e. $\sum_{n\leqq R^2} (1-n/R^2)^\delta B_n(x) \to s$ as $R\to\infty$.

there exists a polynomial $P(t)$, *in* t^2, *of degree* $2(q-1)$ *such that*

$$g_x(t) - P(t) \sim \frac{s t^{2q}\Gamma(\frac{1}{2}k)}{2^{2q} q!\,\Gamma(\frac{1}{2}k + q)},$$

as $t \to +0$.

In section 3 of this paper we obtain, in Theorem 2, a generalization of Theorem A. We also obtain (Theorem 1) a converse result, which is a version of Theorem B applying specifically to multiple Fourier series.

We also extend results recently obtained in [13] and show that the summability, by spherical Riesz means, of a derived multiple Fourier series depends on the behaviour of a certain one-dimensional Fourier series. Known results then enable us (at least when k is odd) to give a complete solution to the spherical summability problem for derived multiple Fourier series.

2. Preliminaries. In this section we summarise known results, obtain some lemmas, and give definitions and notation which, together with that already given in section 1, will be required later.

Bessel Functions. [11]. The Bessel function $J_\mu(t)$, of the first kind and order μ $(\geqq 0)$, is defined by

$$J_\mu(t) = (t/2)^\mu \sum_{\nu=0}^{\infty} (-)^\nu \frac{t^{2\nu}}{2^{2\nu}\nu!\,\Gamma(\nu+\mu+1)}.$$

We write, throughout this paper,

$$V_\mu(t) = t^{-\mu} J_\mu(t) \qquad (t > 0)$$

$$V_\mu(0) = 1.$$

It is known that

$$|V_\mu(t)| \leqq \begin{cases} A(\mu) & 0 \leqq t < 1 \\ A(\mu)t^{-\mu-\frac{1}{2}} & t \geqq 1, \end{cases} \tag{2.1}$$

and that

$$V_\mu'(t) = -tV_{\mu+1}(t). \tag{2.2}$$

Fractional Integrals. For $t > 0$, $\zeta \geqq 1$, $u^{\zeta-1}\phi(u) \in L(0,t)$ we write

$$\left.\begin{aligned} \Phi_{p,\zeta}(t) &= \frac{1}{2^{p-1}\Gamma(p)}\int_0^t (t^2-u^2)^{p-1}u^{\zeta-1}\phi(u)\,du \\ \phi_{p,\zeta}(t) &= \frac{2^p\Gamma(p)}{B(p,\frac{1}{2}\zeta)}t^{-2p-\zeta+2}\Phi_{p,\zeta}(t) \end{aligned}\right\} (p > 0)$$

$$\phi_{0,\zeta}(t) = \Phi_{0,\zeta}(t) = \phi(t),$$

and a similar notation is used when we replace $\phi(u)$ by $g(u)$ etc., with the convention that if $\phi(u)=f_x(u)$ and $\zeta=k$ we write $f_{x,p}(u)$ for $\phi_{p,\zeta}(u)$.

If, for $q\geqq 0$,

$$\Phi_{p,\zeta}(t)\sim\frac{B(p,q+\tfrac{1}{2}\zeta)}{2^p\Gamma(p)}\,st^{2p+2q+\zeta-2}$$

as $t\to+0$ we write[5]

$$\phi(t)\sim st^{2q}(C_\zeta,p)$$

as $t\to+0$.

It is known that[6] if $p\geqq 1$

$$|f_x(t)|=O(1)\,(C_k,p) \tag{2.3}$$

as $t\to\infty$.

Summability by Riesz means. If $\delta\geqq 0$, and if

$$\sum_{n\leqq R^2}(1-n/R^2)^\delta a_n\to s$$

as $R\to\infty$, then $\sum a_n$ is said to be summable (n,δ) to s.

Bochner's Integral. Bochner[7] has shown that if $\delta>\tfrac{1}{2}(k-1)$ then

$$S_R^\delta(f,x)=\frac{2^{\delta-\frac{1}{2}k+1}\Gamma(\delta+1)}{\Gamma(\frac{1}{2}k)}\,R^k\int_0^\infty f_x(t)\,t^{k-1}V_{\delta+\frac{1}{2}k}(tR)\,dt.$$

Since, by (2.3), $|f_x(t)|=O(1)\,(C_k,1)$ as $t\to\infty$ it follows, using (2.1) that

$$\begin{aligned}\Big|\int_\pi^\infty f_x(t)\,t^{k-1}V_{\delta+\frac{1}{2}k}(tR)\,dt\Big| &\leqq AR^{-\delta-\frac{1}{2}k-\frac{1}{2}}\int_\pi^\infty |f_x(t)|\,t^{k-1}\frac{dt}{t^{\delta+\frac{1}{2}k+\frac{1}{2}}}\\ &=AR^{-\delta-\frac{1}{2}k-\frac{1}{2}}\left\{\left[\frac{O(t^k)}{t^{\delta+\frac{1}{2}k+\frac{1}{2}}}\right]_\pi^\infty+\int_\pi^\infty\frac{O(t^k)}{t^{\delta+\frac{1}{2}k+\frac{3}{2}}}\,dt\right\}\\ &=O(R^{-k-\alpha}),\end{aligned}$$

where $\alpha\geqq 0$, provided that $\delta>\alpha+\tfrac{1}{2}k-\tfrac{1}{2}$. Hence, in the case $k=1$,

$$S_R^\delta(f,x)=\frac{2^{\delta+\frac{1}{2}}\Gamma(\delta+1)}{\Gamma(\frac{1}{2})}\,R\int_0^\pi f_x(t)\,V_{\delta+\frac{1}{2}}(tR)\,dt+o(R^{-\beta}), \tag{2.4}$$

where $\beta\geqq 0$, provided that $\delta>\beta$.

---

[5] If $\phi(u)\in L$ this is equivalent to $\phi(t)\sim st^{2q}(C,p)$ see [7].

[6] Bochner [2], page 185, (2.3) means

$$\int_0^t (t^2-u^2)^{p-1}u^{k-1}\,|f_x(u)|\,du=O(t^{2p+k-2})\quad(t\to\infty).$$

[7] Bochner [2] page 176, Formula 10.

We require also the following lemmas.

Lemma 1. *If r is zero or a positive integer, and if $\sum_{n=1}^{\infty} n^r a_n$ is summable $(n, \delta + r)$ $(\delta \geqq 0)$ then $\sum_{n=1}^{\infty} a_n$ is summable (n, δ).*

This follows from the corresponding result, given by Bosanquet,[8] for summability (C), and the equivalence of the Riesz and Cesaro processes.

Lemma 2.[9] *If h is zero or a positive integer, and if*

$$\lambda(u) = \sum_{\nu=q}^{\infty} (-)^{\nu} \frac{u^{2\nu-2q}}{2^{2\nu}\nu!\Gamma(\nu+\mu+1)} \quad (\mu \geqq 0)$$

then

$$\left|\left(\frac{1}{x}\frac{d}{dx}\right)^h \lambda(xt)\right| \leqq \begin{cases} At^{2h} & (0 < x < t^{-1}) \\ At^{2h}[(xt)^{-\mu-2q-h-\frac{1}{2}} + (xt)^{-2h-2}] & (x \geqq t^{-1}), \end{cases}$$

where A is independent of x and t.

Firstly for finite z and t

$$\left(\frac{1}{z}\frac{d}{dz}\right)^h \lambda(z) = \sum_{\nu=q+h}^{\infty} (-)^{\nu} \frac{(2\nu-2q)\cdots(2\nu-2q-2h+2)}{2^{2\nu}\nu!\Gamma(\nu+\mu+1)} z^{2\nu-2q-2h},$$

where the differentiation under the summation sign is justified by the uniform convergence of the resulting series. Hence, for $h = 0, 1, \cdots$, $\left(\frac{1}{z}\frac{d}{dz}\right)^h \lambda(z)$ is regular in the whole plane so that there exists a constant K, independent of z, such that

$$\left|\left(\frac{1}{z}\frac{d}{dz}\right)^h \lambda(z)\right| < K \qquad (|z| < 1). \tag{2.5}$$

Next, for $u > 0$,

$$\lambda(u) = 2^{\mu} u^{-2q} V_{\mu}(u) - P(u)$$

where

$$P(u) = \sum_{\nu=0}^{q-1} (-)^{\nu} \frac{u^{2\nu-2q}}{2^{2\nu}\nu!\Gamma(\nu+\mu+1)}.$$

Now by (2.1) and (2.2), for $u \geqq 1$, $h = 0, 1, \cdots$,

$$\left|\left(\frac{1}{u}\frac{d}{du}\right)^h u^{-2q} V_{\mu}(u)\right| \leqq Au^{-\mu-2q-h-\frac{1}{2}}, \tag{2.6}$$

where A is independent of u. Further, for $u \geqq 1$,

---

[8] Bosanquet [4] page 277, Lemma 3.

[9] Cf. also Shapiro [9], [10].

$$|(\frac{1}{u}\frac{d}{du})^h P(u)| = \begin{cases} |P(u)| & (h=0) \\ |\sum_{\nu=0}^{q-1}(-)^\nu \frac{(2\nu-2q)\cdots(2\nu-2q-2h+2)}{2^{2\nu}\nu!\Gamma(\nu+\mu+1)} u^{2\nu-2q-2h}| & (h=1,2,\cdots) \end{cases} \tag{2.7}$$

$$\leqq Au^{-2h-2} \qquad (h=0,1,\cdots).$$

Combining (2.6) and (2.7) we obtain, for $u \geqq 1$ and $h = 0,1,\cdots$,

$$|(\frac{1}{u}\frac{d}{du})^h \lambda(u)| \leqq Au^{-2q-h-\mu-\frac{1}{2}} + Au^{-2h-2}. \tag{2.8}$$

The required inequalities follow from (2.5) and (2.8).

LEMMA 3. *If* $p > \frac{1}{2}(k+1)$ *then for* $t > 0$ *and all* x,

$$f_{x,p}(t) = 2^{p+\frac{1}{2}(k-2)}\Gamma(p+\tfrac{1}{2}k)\sum_{n=0}^{\infty} A_n(x) V_{p+\frac{1}{2}(k-2)}(t\sqrt{n}).$$

There exists a sequence $\{f^r(x)\}$ $(r=1,2,\cdots)$ of exponential polynomials such that

$$\lim_{r\to\infty} \int_{x_1\cdots x_k=0}^{2\pi}\cdots\int |f(x)-f^r(x)|\,dx_1\cdots dx_k = 0. \tag{2.9}$$

If

$$f^r(x) = \sum_{n=0}^{N_1(r)} b_{n_1\cdots n_k}{}^{(r)} e^{i(n_1x_1+\cdots+n_kx_k)} \tag{2.10}$$

then it follows from (2.9) that

$$\lim_{r\to\infty} b_{n_1\cdots n_k}{}^{(r)} = a_{n_1\cdots n_k} \tag{2.11}$$

uniformly in $(n_1,\cdots,n_k)$ and that, for each fixed positive t and all x

$$\lim_{r\to\infty} f_{x,p}{}^r(t) = f_{x,p}(t). \tag{2.12}$$

If $N_1(r)$ does not tend to infinity with r it follows that $f(x)$ differs from an exponential polynomial only in a set of (k-dimensional) measure zero. In fact in this case the Fourier series of $f(x)$ is finite and we may write

$$f(x) = \sum_{n=0}^{N_0} A_n(x) = \sum_{n=0}^{N_0} a_{n_1\cdots n_k} e^{i(n_1x_1+\cdots+n_kx_k)} \tag{2.13}$$

p. p. in $0 \leqq x_i \leqq 2\pi$ $(i=1,\cdots,k)$. The result stated then follows on taking the spherical mean of order p of both sides of (2.13), since[10] the spherical mean of order p of $e^{i(n_1x_1+\cdots+n_kx_k)}$ is, at the point x,

$$2^{p+\frac{1}{2}(k-2)}\Gamma(p+\tfrac{1}{2}k)V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})e^{i(n_1x_1+\cdots+n_kx_k)}.$$

Now suppose that $N_1(r)\to\infty$ as $r\to\infty$. Taking the spherical mean of order p of both sides of (2.9) we have

$$f_{x,p}{}^{r}(t)=c\sum_{n=0}^{N_1(r)}b_{n_1\cdots n_k}{}^{(r)}e^{i(n_1x_1+\cdots+n_kx_k)}V_{p+\frac{1}{2}(k-2)}(t\sqrt{n}),$$

where $c=2^{p+\frac{1}{2}(k-2)}\Gamma(p+\frac{1}{2}k)$. Consequently, writing

$$T_N=c\sum_{n=0}^{N}a_{n_1\cdots n_k}e^{i(n_1x_1+\cdots+n_kx_k)}V_{p+\frac{1}{2}(k-2)}(t\sqrt{n}),$$

we have, for fixed r and $N>N_1(r)$

$$\begin{aligned}T_N-f_{x,p}(t)&=c\sum_{n=0}^{N_1(r)}(a_{n_1\cdots n_k}-b_{n_1\cdots n_k}{}^{(r)})e^{i(n_1x_1+\cdots+n_kx_k)}V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})\\&\quad+c\sum_{n=N_1(r)+1}^{N}a_{n_1\cdots n_k}e^{i(n_1x_1+\cdots+n_kx_k)}V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})\\&\quad+f_{x,p}{}^{r}(t)-f_{x,p}(t).\end{aligned}\tag{2.14}$$

Since $a_{n_1\cdots n_k}=o(1)$ as $(n_1,\cdots,n_k)\to(\infty,\cdots,\infty)$ and since the number of points $(n_1,\cdots,n_k)$ for which $n_1{}^2+\cdots+n_k{}^2=n$ is $O(n^{\frac{1}{2}k+\zeta-1})$ where $\zeta(>0)$ is arbitrary, it follows from (2.1) that $\sum_{n=0}^{\infty}a_{n_1\cdots n_k}V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})$ is absolutely convergent for fixed $t(>0)$ provided that $p>\frac{1}{2}(k+1)+2\zeta$. Hence, from (2.1), (2.11), (2.12) and (2.14), for fixed $t(>0)$ and all x,

$$\begin{aligned}\overline{\lim_{N\to\infty}}\,|T_N-f_{x,p}(t)|&\leqq c\sum_{n=0}^{N_1(r)}|a_{n_1\cdots n_k}-b_{n_1\cdots n_k}{}^{(r)}|\,|V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})\\&\quad+c\sum_{N_1(r)+1}^{\infty}|a_{n_1\cdots n_k}|\,|V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})|\\&\quad+|f_{x,p}{}^{r}(t)-f_{x,p}(t)|\\&=o\{\sum_{n=1}^{\infty}n^{\frac{1}{2}k+\zeta-1}|V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})|\}\\&\quad+O\{\sum_{N_1(r)+1}^{\infty}n^{\frac{1}{2}k+\zeta-1}|V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})|\}\\&\quad+o(1)\\&=o(1)\end{aligned}$$

as $r\to\infty$, provided that $p>\frac{1}{2}(k+1)+2\zeta$.

---

[10] See, for example, [6] page 694, Formula 10.

Hence

$$\lim_{N\to\infty} T_N = f_{x,p}(t),$$

for fixed positive t and all x provided that $p > \frac{1}{2}(k+1) + 2\zeta$. Since $\zeta(>0)$ is arbitrary the result stated follows immediately.

It is perhaps worth remarking that Lemma 3 may be put into a different form. We have, for $p > \frac{1}{2}(k+1)$ and $t > 0$,

$$\begin{aligned} f_{x,p}(t) &= c \lim_{N\to\infty} \sum_{n=0}^{N} A_n(x) V_{p+\frac{1}{2}(k-2)}(t\sqrt{n}) \\ &= c \lim_{N\to\infty} \{ \sum_{n=0}^{N} S_{\sqrt{n}}(f,x) \Delta[V_{p+\frac{1}{2}(k-2)}(t\sqrt{n})] \\ &\qquad + S_{\sqrt{N}}(f,x) V_{p+\frac{1}{2}(k-2)}(t\sqrt{N}) \} \end{aligned}$$

where $S_R(f,x) = S_R{}^0(f,x) = \sum_{n \leqq R^2} A_n(x)$.

Hence, since $S_R(f,x) = O(R^{k+\zeta})$ (where $\zeta(>0)$ is arbitrary) it follows, using (2.1) that for fixed $t(>0)$

$$\begin{aligned} f_{x,p}(t) &= c \lim_{N\to\infty} \{ t^2 \int_0^{\sqrt{N}} R S_R(f,x) V_{p+\frac{1}{2}(k-2)+1}(tR)\, dR \\ &\qquad + \frac{o(N^{\frac{1}{2}k+\frac{1}{2}\zeta})}{N^{\frac{1}{2}(p+\frac{1}{2}k-\frac{1}{2})}} \} \\ &= ct^2 \int_0^{\infty} R S_R(f,x) V_{p+\frac{1}{2}k}(tR)\, dR, \end{aligned}$$

provided that $p > \frac{1}{2}(k+1)$. In this form Lemma 3 has been obtained by Chandrasekharan[11] with the condition $p > \frac{1}{2}(k+1)$ replaced by $p > \frac{1}{2}(k+3)$.

3. We suppose, throughout the rest of this paper, that q is a positive integer and that

$$g(t) = \frac{2^{2q} q!\, \Gamma(q+\frac{1}{2}k)}{\Gamma(\frac{1}{2}k)} \{ f_{x^0}(t) - \Gamma(\tfrac{1}{2}k) \sum_{\nu=0}^{q-1} \frac{a_\nu t^{2\nu}}{2^{2\nu} \nu!\, \Gamma(\nu+\frac{1}{2}k)} \} \quad (t > 0),$$

where the a_ν $(\nu = 0, \cdots, q-1)$ are independent of t, and x^0 is some given point.

We first obtain

---

[11] [6] page 996, Lemma 2, the case $\delta = 0$. Another form of this lemma is given in [5] p. 216 (and is reproduced in [7] p. 135) but the proof of this version appears to be invalid.

THEOREM 1. *If* $(-)^q \sum_{n=1}^{\infty} n^q A_n(x^0)$ *is summable* $(n, \delta + 2q)$ $(\delta \geqq 0)$ *to* s *then there exist constants* a_ν *such that*

$$g(t) \sim st^{2q}\,(C_k, p), \tag{3.1}$$

as $t \to +0$, *whenever* $p > \max[\delta - \tfrac{1}{2}(k-3), \tfrac{1}{2}(k+1)]$.

Moreover, for $\nu = 0, 1, \cdots, q-1$,

$$a_\nu = (-)^\nu \lim_{R\to\infty} \sum_{n \leqq R^2} (1 - n/R^2)^{\delta+q+\nu} n^\nu A_n(x^0). \tag{3.2}$$

We may suppose, without loss of generality, that $s = 0$. For if, in particular, $f(x) = (-)^q s e^{i(x_1 + \cdots + x_k)}$ and $x^0 = (0, \cdots, 0)$ then[12] the derived series (1.1) consists of the single term $se^{i(x_1+\cdots+x_k)}$ which converges to s at $x = x^0$. Moreover, if $a_\nu = (-)^{\nu+q}s$ then the a_ν satisfy (3.2). Since the spherical mean at $x = x^0$ of $(-)^q s e^{i(x_1+\cdots+x_k)}$ is $(-)^q s 2^{\frac{1}{2}(k-2)}\Gamma(\tfrac{1}{2}k) V_{\frac{1}{2}(k-2)}(t)$ it follows that, in this case,

$$\begin{aligned} g(t) &= 2^{2q} q\,!\,\Gamma(q + \tfrac{1}{2}k)\Big\{(-)^q s 2^{\frac{1}{2}(k-2)} V_{\frac{1}{2}(k-2)}(t) - \sum_{\nu=0}^{q-1} \frac{(-)^{\nu+q} t^{2q} s}{2^{2\nu}\nu\,!\,\Gamma(\nu + \frac{1}{2}k)}\Big\} \\ &= st^{2q} + (-)^q s 2^{2q} q\,!\,\Gamma(q + \tfrac{1}{2}k) \sum_{\nu=q+1}^{\infty} (-)^\nu \frac{t^{2\nu}}{2^{2\nu}\nu\,!\,\Gamma(\nu + \frac{1}{2}k)} \\ &\sim st^{2q}, \end{aligned}$$

as $t \to +0$. Hence, if $f(x)$ is replaced by $f(x) - (-)^q s e^{i(x_1 - x_1^0 + \cdots + x_k - x_k^0)}$, s is replaced by zero.

Writing

$$T(0, u) = \sum_{1 \leqq n \leqq u^2} n^q A_n(x^0)$$

$$T(m, u) = \int_1^u yT(m-1, y)\,dy \qquad (m = 1, 2, \cdots)$$

we note that since $A_n(x^0) = O(n^{\frac{1}{2}k-1+\zeta})$ where $\zeta (> 0)$ is arbitrary

$$T(m, u) = O(u^{2m+2q+2\zeta+k}) \qquad (m = 0, 1, \cdots). \tag{3.3}$$

Writing also, for simplicity, $\tau = \delta + 2q$, $\mu = p + \tfrac{1}{2}(k-2)$,

$$\left.\begin{aligned} \gamma(t) &= 2^\mu t^{-2q} V_\mu(t) \\ \Gamma(\mu + 1)\phi(t) &= f_{x^0, p}(t) - A_0 \end{aligned}\right\} \tag{3.4}$$

it follows from Lemma 3, (2.6) and (3.3) that, for fixed $t > 0$,

---

[12] For a similar argument see Bosanquet [4] Lemma 8.

$$\begin{aligned}\phi(t) &= t^{2q}\sum_{n=1}^{\infty} n^q A_n(x^0)\gamma(t\sqrt{n}) \\ &= t^{2q}\lim_{y\to+0}\lim_{R\to\infty}\sum_{n=1}^{R} n^q A_n(x^0)e^{-ny}\gamma(t\sqrt{n}) \\ &= t^{2q}\lim_{y\to+0}\lim_{R\to\infty}\{-\int_1^{\sqrt{R}} uT(0,u)\left(\frac{1}{u}\frac{d}{du}\right)e^{-u^2y}\gamma(ut)\,du \\ &\qquad\qquad + T(0,\sqrt{R})e^{-Ry}\gamma(t\sqrt{R})\} \\ &= t^{2q}\lim_{y\to+0}\lim_{R\to\infty}\{\sum_{m=0}^{h+1}(-)^{m+1}[T(m,u)\left(\frac{1}{u}\frac{d}{du}\right)^m e^{-u^2y}\gamma(ut)]_{u=\sqrt{R}} \\ &\qquad\qquad + (-)^h\int_1^{\sqrt{R}} uT(h+1,u)\left(\frac{1}{u}\frac{d}{du}\right)^{h+2}e^{-u^2y}\gamma(ut)\,du\} \\ &= (-)^h t^{2q}\lim_{y\to+0}\int_1^{\infty} uT(h+1,u)\left(\frac{1}{u}\frac{d}{du}\right)^{h+2}e^{-u^2y}\gamma(ut)\,du \\ &= (-)^h t^{2q}\lim_{y\to+0}\sum_{\nu=0}^{h+2}\binom{h+2}{\nu}(-2y)^{\nu}\int_1^{\infty} uT(h+1,u)e^{-u^2y}\left(\frac{1}{u}\frac{d}{du}\right)^{h+2-\nu}\gamma(ut)\,du.\end{aligned}\tag{3.5}$$

We now choose h to be the *greatest integer less than* τ. Then since[18] $T(h+1,u) = cu^{2h+2}\Delta_{x^0}{}^q S_u{}^{h+1}(f,x^0)$ it follows by consistency that $T(h+1,u) = o(u^{2h+2})$ and hence, using (2.6), that for $\nu = 1, 2, \cdots, h+2$ and fixed $t(>0)$,

$$\begin{aligned}&\int_1^{\infty} uT(h+1,u)e^{-u^2y}\left(\frac{1}{u}\frac{d}{du}\right)^{h+2-\nu}\gamma(ut)\,du \\ &= \int_1^{\infty} e^{-u^2y}o(u^{h-\mu-2q+\nu+\frac{1}{2}})\,du \\ &= o(y^{-\nu}),\end{aligned}$$

as $y\to+0$, if $p > \delta - \frac{1}{2}(k-3)$. Hence from (3.5), if

$$p > \max[\delta - \tfrac{1}{2}(k-3), \tfrac{1}{2}(k+1)],$$

$$\phi(t) = (-)^h t^{2q}\lim_{y\to+0}\int_1^{\infty} uT(h+1,u)e^{-u^2y}\left(\frac{1}{u}\frac{d}{du}\right)^{h+2}\gamma(ut)\,du. \tag{3.6}$$

We now write, as in Lemma 2,

$$\lambda(u) = \sum_{\nu=q}^{\infty}(-)^{\nu}\frac{u^{2\nu-2q}}{2^{2\nu}\nu!\Gamma(\nu+\mu+1)}$$

$$P(u) = \sum_{\nu=0}^{q-1}(-)^{\nu}\frac{u^{2\nu-2q}}{2^{2\nu}\nu!\Gamma(\nu+\mu+1)},$$

---

[18] Throughout what follows $c_0, c_1, c_2, \cdots$ denote constants not necessarily the same at each occurrence.

and

$$\left(\frac{1}{u}\frac{d}{du}\right)^{h+2} P(u) = \sum_{\nu=0}^{q-1} b_\nu u^{+2\nu-2q-2h-4}$$

where

$$(3.7) \qquad b_\nu = (-)^\nu \frac{(2\nu-2q)\cdots(2\nu-2q-2h-2)}{2^{2\nu}\nu!\Gamma(\nu+\mu+1)}$$

Substituting the relation

$$\gamma(u) = P(u) + \lambda(u)$$

in (3.6) we obtain

$$(3.8) \qquad \begin{aligned} \phi(t) &= \sum_{\nu=0}^{q-1} c_\nu t^{2\nu} + (-)^h t^{2q} \lim_{y\to+0} \int_1^\infty uT(h+1,u)e^{-u^2y}\left(\frac{1}{u}\frac{d}{du}\right)^{h+2}\lambda(ut)\,du \\ &= \sum_{\nu=0}^{q-1} c_\nu t^{2\nu} + t^{2q} I(t) \end{aligned}$$

say, where for $\nu = 0, 1, \cdots, q-1$,

$$(3.9) \qquad \begin{aligned} c_\nu &= (-)^h b_\nu \lim_{y\to+0} \int_1^\infty T(h+1,u)e^{-u^2y}u^{2\nu-2q-2h-3}\,du \\ &= (-)^h b_\nu \int_1^\infty T(h+1,u)u^{2\nu-2q-2h-3}\,du \end{aligned}$$

since $(T(h+1,u) = O(u^{2h+2}))$ this last integral is absolutely convergent.

We first show that

$$(3.10) \qquad I(t) = O(1),$$

as $t \to +0$.

If τ is an integer, then $\tau = h+1$ and so by Lemma 2,

$$\begin{aligned} I(t) &= (-)^{\tau-1} \lim_{y\to+0} \int_1^\infty uT(\tau,u)e^{-u^2y}\left(\frac{1}{u}\frac{d}{du}\right)^{\tau+1}\lambda(ut)\,du \\ &= (-)^{\tau-1} \int_1^\infty uT(\tau,u)\left(\frac{1}{u}\frac{d}{du}\right)^{\tau+1}\lambda(ut)\,du \\ &= O\left(t^{2\tau+2}\int_1^{t^{-1}} u^{2\tau+1}\,du\right) + O\left(\int_{t^{-1}}^\infty u^{2\tau+1}t^{2\tau+2}\left[(ut)^{-\mu-2q-\tau-\frac{3}{2}} + (ut)^{-2\tau-4}\right]du\right) \\ &= O(1) \end{aligned}$$

as $t \to +0$ provided that $p > \delta - \frac{1}{2}(k-3)$.

If τ is not an integer, we write

$$T(h+1,u) = c\int_1^u (u^2-v^2)^{h-\tau} vT(\tau,v)\,dv$$

where c is independent of u. We then substitute this expression into the integral defining $I(t)$ and invert the order of integration. Estimating the inner integral by standard methods then leads to (3.10).[14]

Collecting results we have, from (3.8),

$$\phi(t) = \sum_{\nu=0}^{q-1} c_\nu t^{2\nu} + O(t^{2q})$$

i.e., using (3.4), that

$$f_{x^0,p}(t) = \Gamma(\mu+1) \sum_{\nu=0}^{q-1} \frac{a_\nu t^{2\nu}}{2^{2\nu}\nu\,!\Gamma(\nu+\mu+1)} + O(t^{2q})$$

where

$$a_\nu = c_\nu 2^{2\nu}\nu\,!\Gamma(\nu+\mu+1) \qquad (\nu = 1,\cdots,q-1)$$

$$a_0 = c_0 + A_0/\Gamma(\mu+1).$$

Now

$$g_{p,k}(t) = \frac{2t^{-2p-k+2}}{B(p,\tfrac{1}{2}k)} \int_0^t (t^2-u^2)^{p-1}u^{k-1}g(u)\,du$$

so that

$$\frac{\Gamma(\tfrac{1}{2}k)}{2^{2q}q\,!\Gamma(q+\tfrac{1}{2}k)} g_{p,k}(t)$$

$$= \frac{2t^{-2p-k+2}\Gamma(p+\tfrac{1}{2}k)}{\Gamma(\tfrac{1}{2}k)\Gamma(p)} \int_0^t (t^2-u^2)^{p-1}u^{k-1}\{f_{x^0}(u) - \Gamma(\tfrac{1}{2}k)\sum_{\nu=0}^{q-1}\frac{a_\nu u^{2\nu}}{2^{2\nu}\nu\,!\Gamma(\nu+\tfrac{1}{2}k)}\}\,du$$

$$= f_{x^0,p}(t) - \Gamma(\mu+1)\sum_{\nu=0}^{q-1}\frac{a_\nu t^{2\nu}}{2^{2\nu}\nu\,!\Gamma(\nu+\mu+1)}$$

$$= O(t^{2q})$$

as $t \to +0$.

We have thus shown that if $(-)^q \sum_{n=1}^{\infty} n^q A_n(x^0)$ is summable $(n, \delta+2q)$ to s then there exist constants a_ν such that (3.1) is satified for

$$p > \max[\delta - \tfrac{1}{2}(k-3), \tfrac{1}{2}(k+1)].$$

It remains to show that the a_ν, which are clearly unique, satisfy (3.2).

It follows from Lemma 1 that $(-)^{q-1}\sum_{n=0}^{\infty} n^{q-1}A_n(x^0)$ is summable $(n, \delta+2q-1)$, i.e. that

$$(-)^{q-1}\lim_{R\to\infty}\sum_{n\leqq R^2}(1-n/R^2)^{\delta+2q-1}n^{q-1}A_n(x^0) = s',$$

---

[14] We omit the details, which are rather tedious. We shall only *use* Theorem 1 in the case when τ is an integer. The method outlined here is a combination of those in [5] page 215, Verblunsky [11], and [3].

say. From what we have already proved (with q replaced by $q-1$) there exist constants a_ν' such that

$$\frac{2^{2q-2}(q-1)!\Gamma(q-1+\tfrac{1}{2}k)}{\Gamma(\tfrac{1}{2}k)}\{f_{x^0}(t)-\Gamma(\tfrac{1}{2}k)\sum_{\nu=0}^{q-2}\frac{a_\nu' t^{2\nu}}{2^{2\nu}\nu!\Gamma(\nu+\tfrac{1}{2}k)}\}$$
$$\sim s' t^{2q-2}(C_k)$$

as $t\to+0$. However we have just shown that

$$\frac{2^{2q}q!\Gamma(q+\tfrac{1}{2}k)}{\Gamma(\tfrac{1}{2}k)}\{f_{x^0}(t)-\Gamma(\tfrac{1}{2}k)\sum_{\nu=0}^{q-2}\frac{a_\nu t^{2\nu}}{2^{2\nu}\nu!\Gamma(\nu+\tfrac{1}{2}k)}$$
$$=g(t)+a_{q-1}\frac{t^{2q-2}2^{2q}q!\Gamma(q+\tfrac{1}{2}k)}{2^{2q-2}(q-1)!\Gamma(q-1+\tfrac{1}{2}k)}$$
$$\sim st^{2q}(C_k)+a_{q-1}\frac{t^{2q-2}2^{2q}q!\Gamma(q+\tfrac{1}{2}k)}{2^{2q-2}(q-1)!\Gamma(q-1+\tfrac{1}{2}k)}$$
$$\sim a_{q-1}t^{2q-2}\frac{2^{2q}q!\Gamma(q+\tfrac{1}{2}k)}{2^{2q-2}(q-1)!\Gamma(q-1+\tfrac{1}{2}k)}(C_k)$$

as $t\to+0$. Hence $a_\nu=a_\nu'$ $(\nu=0,1,\cdots,q-2)$ and $a_{q-1}=s'$ i.e.

$$a_{q-1}=(-)^{q-1}\lim_{R\to\infty}\sum_{n\leqq R^2}(1-n/R^2)^{\delta+2q-1}n^{q-1}A_n(x^0).$$

Repetition of this argument shows that all the a_ν satisfy (3.2).

We next obtain a theorem which is converse to Theorem 1.

THEOREM 2. *If constants a_ν exist such that*

$$(3.11)\qquad g(t)\sim st^{2q}(C_k,p)\quad(p\geqq 0)$$

as $t\to+0$ then $(-)^q\sum_{n=1}^{\infty}n^qA_n(x^0)$ is summable $(n,\delta+2q)$ to s whenever $\delta>p+\tfrac{1}{2}(k-1)$.

Moreover the constants a_ν are given by (3.2).

We observe first that we may suppose, without loss of generality that $s=a_\nu=0$ $(\nu=0,1,\cdots,q-1)$. For in the case

$$f(x)-P(x)=\sum_{\nu=0}^{q}a_\nu\{\frac{(x_1{}^0-x_1)^{2\nu}+\cdots+(x_k{}^0-x_k)^{2\nu}}{(2\nu)!}\}$$
$$(x_i{}^0\leqq x_i\leqq x_i{}^0+2\pi;\ i=1,\cdots,k)$$

where $a_q=s$, it follows from a known theorem[15] that $(-)^\nu\sum_{n=1}^{\infty}n^\nu A_n(x^0)$ is summable $(n,\delta+2\nu)$ $(\delta>\tfrac{1}{2}(k-1)$ to a_ν at $x=x^0$ $(\nu=0,\cdots,q)$.

---

[15] [7] page 124, Theorem 4.62.

Moreover in this case[16] $g(t) = st^{2q}$ $(0 < t < \pi)$ so that if $f(x) \equiv P(x)$ then for any $p \geqq 0$ (3.11) is satisfied, the conclusion of Theorem 2 is satisfied and the a_ν satisfy (3.2) so that by considering $f(x) - P(x)$ in place of $f(x)$ we may suppose $s = 0 = a_\nu$ $(\nu = 0, \cdots, q-1)$.

We may thus suppose that

$$f_{x^0,p}(t) = o(t^{2q}) \tag{3.12}$$

as $t \to +0$.

Next[17]

$$\Delta_{x^0}{}^q S_R{}^{\delta+2q}(f, x^0) = R^{2q} \sum_{\nu=0}^{q} c_\nu S_R{}^{\delta+2q+\nu}(f, x^0) \tag{3.13}$$

where the c_ν $(\nu = 0, \cdots, q)$ are independent of R. Hence it is sufficient to show that

$$S_R{}^{\delta+2q+\nu}(f, x^0) = O(R^{-2q}) \qquad (\nu = 0, \cdots, q).$$

From a known result[18]

$$S_R{}^{\delta+2q+\nu}(f, x^0) = cR^{2p+k} \int_0^\infty f_{x^0,p}(t)\, t^{k+2p-1} V_{\delta+2q+\nu+p+\frac{1}{2}k}(tR)\, dt \tag{3.14}$$

provided that $\delta > p + \frac{1}{2}(k-1)$. Consequently, from (3.12) and (2.1),

$$\begin{aligned} R^{2q} S_R{}^{\delta+2q+\nu}(f, x^0) &= o\left(R^{2p+k+2q} \int_0^{R^{-1}} t^{k+2p+2q-1}\, dt\right) \\ &\quad + o\left(\int_{R^{-1}}^{\infty} \frac{R^{2p+k+2q} t^{k+2q+2p-1}}{(tR)^{\delta+2q+\nu+\frac{1}{2}k+p+\frac{1}{2}}}\, dt\right) \\ &= O(1) \end{aligned}$$

as $R \to \infty$ provided that $\delta > p + \frac{1}{2}(k-1)$.

Finally it follows from Theorem 1 that, since $(-)^q \sum_{n=1}^{\infty} n^q A_n(x^0)$ is summable $(n, \delta + 2q)$ to s, the a_ν are given by (3.2).

4. Throughout this section we suppose that $h(t)$ is an even periodic function with period 2π which coincides with $t^{k-1}g(t)$ in $0 < t < \pi$ and that

$$h(t) \sim \tfrac{1}{2} b_0 + \sum_{n=1}^{\infty} b_n \cos nt.$$

The main result of this section may then be formulated as follows.

---

[16] It is easy to verify that in this case

$$f_{x^0}(t) = \Gamma(\tfrac{1}{2}k) \sum_{\nu=0}^{q} \frac{a_\nu t^{2\nu}}{2^{2\nu} \nu! \Gamma(\nu + \frac{1}{2}k)}.$$

[17] [9] page 227.

[18] [10] page 214.

THEOREM 3. *If* $\delta > \frac{1}{2}(k-1)$ $(k > 1)$ *and* q *is a positive integer then* $(-)^q \sum_{n=1}^{\infty} n^q A_n(x^0)$ *is summable* $(n, \delta + 2q)$ *to* s *if and only if there exist constants* a_ν $(\nu = 0, \cdots, q-1)$ *such that* (i)[19] $g(t) \sim st^{2q}(C_k)$ *as* $t \to +0$ *and* (ii) *if* k *is odd* $\sum_{n=1}^{\infty} n^{2q+k-1} b_n$ *is summable* $(C, \delta + 2q + \frac{1}{2}k - \frac{1}{2})$ *to* $(-)^{\frac{1}{2}(k-1)+q}(2q+k-1)!s$ *or* (ii)′ *if* k *is even*

$$n^{2q+k} b_n \to (-)^{\frac{1}{2}k+q}(2q+k-1)!\,2s/\pi\,(C, \delta + 2q + \tfrac{1}{2}k + \tfrac{1}{2})$$

as $n \to \infty$.

The a_ν, *when they exist are given by* (3.2).

We require two further lemmas.

LEMMA 4. *If* $\delta > \frac{1}{2}(k-1)$ *then*

$$R^{k+2q} \int_{\pi}^{\infty} g(t)\, t^{k-1} V_{\delta+2q+\frac{1}{2}k}(tR)\, dt = O(1)$$

as $R \to \infty$. *The same is true if* $g(t)$ *is replaced by* t^{2q}.

Since, by (2.3), as $t \to \infty$,

$$\begin{aligned} |g(t)| &\leqq c\{|f_{x^0}(t)| + \Gamma(\tfrac{1}{2}k) \sum_{\nu=0}^{q-1} \frac{|a_\nu|\, t^{2\nu}}{2^{2\nu}\nu!\,\Gamma(\nu+\frac{1}{2}k)}\} \\ &= O(1)(C_k, 1) + O(t^{2q-2}) \\ &= O(t^{2q-2})(C_k, 1) \end{aligned}$$

it follows, using (2.1) that

$$\begin{aligned} \left| \int_{\pi}^{\infty} g(t)\, t^{k-1} V_{\delta+2q+\frac{1}{2}k}(tR)\, dt \right| &\leqq cR^{-\delta-2q-\frac{1}{2}k-\frac{1}{2}} \int_{\pi}^{\infty} |g(t)|\, t^{k-1} \frac{dt}{t^{\delta+2q+\frac{1}{2}k+\frac{1}{2}}} \\ &= R^{-\delta-2q-\frac{1}{2}k-\frac{1}{2}} \left\{ \left[\frac{O(t^{k+2q-2})}{t^{\delta+2q+\frac{1}{2}k+\frac{1}{2}}} \right]_{\pi}^{\infty} + \int_{\pi}^{\infty} \frac{O(t^{k+2q-2})\, dt}{t^{\delta+2q+\frac{1}{2}k+\frac{3}{2}}} \right\} \\ &= o(R^{-2q-k}) \end{aligned}$$

as $R \to \infty$, since $\delta > \frac{1}{2}(k-1)$.

Finally, by (2.1)

$$\begin{aligned} \left| \int_{\pi}^{\infty} t^{2q+k-1} V_{\delta+2q+\frac{1}{2}k}(tR)\, dt \right| &\leqq cR^{-\delta-2q-\frac{1}{2}k-\frac{1}{2}} \int_{\pi}^{\infty} t^{-\delta+\frac{1}{2}k-\frac{3}{2}}\, dt \\ &= O(R^{-2q-k}) \end{aligned}$$

if $\delta > \frac{1}{2}(k-1)$.

---

[19] Equivalently $(-)^q \sum n^q A_n(x^0)$ is summable by Riesz means of some order to s.

LEMMA 5. *In order that* $(-)^q\sum n^q A_n(x^0)$ *be summable* $(n,\delta+2q)$ $(\delta>\frac{1}{2}(k-1))$ *to* s *it is necessary and sufficient that there exist* a_ν *such that* (i) $g(t)\sim st^{2q}(C_k)$ *as* $t\to+0$ *and* (ii)

$$R^{2q+k}\int_0^\infty g(t)t^{k-1}V_{\delta+2q+\frac{1}{2}k}(tR)\,dt\to\frac{s\Gamma(q+\frac{1}{2}k)}{2^{\delta-\frac{1}{2}k+1}\Gamma(\delta+q+1)}$$

as $R\to\infty$.

Necessity. Suppose that $(-)^q\sum n^q A_n(x^0)$ is summable $(n,\delta+2q)$ to s. It follows from Theorem 1 that constants a_ν exist such that $g(t)\sim st^{2q}(C_k)$ as $t\to+0$. If

$$P(x)=\sum_{\nu=0}^{q}a_\nu\{\frac{(x_1-x_1^0)^{2\nu}+\cdots+(x_k-x_k^0)^{2\nu}}{(2\nu)!}\}\ (a_q=s)$$

$$(x_i^0\leqq x_i\leqq x_i^0+2\pi;\, i=1,\cdots,k)$$

then, as in the working for Theorem 2, when $f(x)=P(x)$ the a_ν satisfy (3.2) and $(-)^q\sum n^q A_n(x^0)$ is summable $(n,\delta+2q)$ $(\delta>\frac{1}{2}(k-1))$ to s. Moreover, since $g(t)=st^{2q}$ $(0<t<\pi)$ it follows that (i) is satisfied. Condition (ii) is satisfied since, using Lemma 4,

$$\begin{aligned}
&R^{k+2q}\int_0^\infty g(t)t^{k-1}V_{\delta+2q+\frac{1}{2}k}(tR)\,dt\\
&\qquad=R^{k+2q}\int_0^\pi g(t)t^{k-1}V_{\delta+2q+\frac{1}{2}k}(tR)\,dt+o(1)\\
&\qquad=sR^{k+2q}\int_0^\pi t^{2q+k-1}V_{\delta+2q+\frac{1}{2}k}(tR)\,dt+o(1)\\
&\qquad=sR^{k+2q}\int_0^\infty t^{2q+k-1}V_{\delta+2q+\frac{1}{2}k}(tR)\,dt+o(1)\\
&\qquad=\frac{s\Gamma(q+\frac{1}{2}k)\ \text{[20]}}{2^{\delta-\frac{1}{2}k+1}\Gamma(\delta+q+1)}+O(1).
\end{aligned}$$

Hence by subtracting $P(x)$ from $f(x)$ we may suppose that $s=a_\nu=0$ $(\nu=0,\cdots,q-1)$, i.e. it is sufficient to prove that

$$(4.1)\qquad R^{2q+k}\int_0^\infty f_{x^0}(t)t^{k-1}V_{\delta+2q+\frac{1}{2}k}(tR)\,dt=o(1)$$

as $R\to\infty$.

We observe that, by Bochner's formula, (4.1) is equivalent to

$$(4.2)\qquad R^{2q}S_R^{\delta+2q}(f,x^0)=o(1)$$

as $R\to\infty$.

---

[20] [11] page 994, Formula 10.

Since $f_{x^0}(t) = O(t^{2q})\,(C_k)$ as $t \to +0$ it follows, as in the working for Theorem 2 that, for some τ_0,

$$R^{2q} S_R^{\tau+2q}(f, x^0) = O(1) \qquad (\tau \geqq \tau_0) \tag{4.3}$$

as $R \to \infty$. Further, by (3.13),

$$\Delta_{x^0}{}^q S_R^{\tau+2q}(f, x^0) = \sum_{\nu=0}^{q} c_\nu R^{2q} S_R^{\tau+2q+\nu}(f, x^0). \tag{4.4}$$

Since, by hypothesis, the left hand side of (4.4) is $O(1)$ as $R \to \infty$ when $\tau = \delta$ it follows by successive applications of (4.3), (4.4) and the consistency of Riesz means that (4.2) is satisfied.

Sufficiency. We may suppose, as before that $a_\nu = s = 0$ $(\nu = 0, 1, \cdots, q-1)$ and that (4.1), or equivalently (4.2), holds. The result then follows, by consistency from (4.4) with τ replaced by δ.

Proof of Theorem 3.[21] Firstly, we may suppose that $s = 0$. For in the case when

$$f(x) = P(x) = s\{\frac{(x_1 - x_1^0)^{2q} + \cdots + (x_k - x_k^0)^{2q}}{(2q)!}\}$$
$$(x_i^0 \leqq x_i \leqq x_i^0 + 2\pi;\ i = 1, \cdots, k)$$

we have, by arguments similar to those used in Theorem 2, that $(-)^q \sum n^q A_n(x^0)$ is summable $(n, \delta + 2q)$ $(\delta > \frac{1}{2}(k-1)$ to s, and if we put $a_\nu = 0$ $(\nu = 0, 1, \cdots, q-1)$ that the a_ν satisfy (3.2). Moreover in this case, for $0 < t < \pi$, $g(t) = st^{2q}$. Hence, if k is odd, $(-)^{q+\frac{1}{2}(k-1)} \sum_{n=1}^{\infty} n^{2q+k-1} b_n$ is the $(2q + k - 1)$-th derived Fourier cosine series at $t = 0$ of st^{2q+k-1} and is therefore summable $(C, \delta + 2q + \frac{1}{2}k - \frac{1}{2})$ to $(2q + k - 1)!s$ whenever $\delta > \frac{1}{2}(k-1)$ ((14), p. 60). On the other hand if k is even a straightforward calculation of the Fourier cosine coefficients b_n of $s\,|\,t^{2q+k-1}\,|$ shows that $n^{2q+k} b_n \to (-)^{\frac{1}{2}k+q} (2q + k - 1)!2s/\pi$, $(C, \delta + 2q + \frac{1}{2}k + \frac{1}{2})$ $(\delta > \frac{1}{2}(k-1))$. Thus when $f(x) = P(x)$, $(-)^q \sum n^q A_n(x^0)$ is summable $(n, \delta + 2q)$ to s for any $\delta > \frac{1}{2}(k-1)$ and (i), (ii) or (ii)′ are satisfied. Hence if we consider $f(x) - P(x)$ in place of $f(x)$ we may suppose that $s = 0$.

Necessity. The case k odd. We suppose that k is odd, $\delta > \frac{1}{2}(k-1)$ and $(-)^q \sum n^q A_n(x^0)$ is summable $(n, \delta + 2q)$ to 0. It follows from Lemma 5 that constants a_ν $(\nu = 0, 1, \cdots, q-1)$ (satisfying (3.2)) exist such that $g(t) = O(t^{2q})\,(C_k)$ as $t \to +0$, i.e. that (i) is satisfied, and that

$$R^{2q+k} \int_0^\infty g(t)\, t^{k-1} V_{\delta+2q+\frac{1}{2}k}(tR)\, dt = o(1)$$

---

[21] The proof of this theorem is similar to that of Theorem 1 of [13], we give brief details for completeness.

as $R \to \infty$, and hence by Lemma 4 that

$$R^{2q+k}\int_0^{\pi} g(t)\, t^{k-1} V_{\delta+2q+\frac{1}{2}k}(tR)\, dt = o(1) \tag{4.5}$$

as $R \to \infty$.

Now by (2.4), with $\beta = 2q + k - 1$ and δ replaced by $\delta + 2q + \frac{1}{2}k - \frac{1}{2}$, f by h we have

$$\begin{aligned} R^{2q+k-1} S_R{}^{\delta+2q+\frac{1}{2}k-\frac{1}{2}}(h,0) &= cR^{2q+k}\int_0^{\pi} h(t)\, V_{\delta+2q+\frac{1}{2}k}(tR)\, dt + o(1) \\ &= o(1), \end{aligned} \tag{4.6}$$

by (4.5).

But, since k is odd,

$$(1 - n^2/R^2)^{\delta+2q+\frac{1}{2}k-\frac{1}{2}} (n^2/R^2)^{q+\frac{1}{2}(k-1)} = \sum_{\nu=0}^{q+\frac{1}{2}(k-1)} c_\nu (1 - n^2/R^2)^{\delta+2q+\frac{1}{2}(k-1)+\nu},$$

so that

$$\begin{aligned} \sum_{n \leqq R} (1 - n^2/R^2)^{\delta+2q+\frac{1}{2}(k-1)} n^{2q+k-1} b_n &= \sum_{\nu=0}^{q+\frac{1}{2}(k-1)} c_\nu R^{2q+k-1} S_R{}^{\delta+2q+\frac{1}{2}(k-1)+\nu}(h,0) \\ &= o(1) \end{aligned} \tag{4.7}$$

as $R \to \infty$, by (4.6) and consistency; equivalently $\sum n^{2q+k-1} b_n$ is summable $(C, \delta + 2q + \frac{1}{2}k - \frac{1}{2})$ to zero.

The case k even. This is proved in a similar way (cf. (13)) and we omit the details.

Sufficiency. The case k odd. Suppose that there exist constants a_ν $(\nu = 0, \cdots, q-1)$ such that $g(t) = O(t^{2q})\,(C_k)$, and that $\sum n^{2q+k-1} b_n$ is summable $(C, \delta + 2q + \frac{1}{2}k - \frac{1}{2})$ to zero or equivalently that

$$\sum_{n<R} (1 - n^2/R^2)^{\delta+2q+\frac{1}{2}(k-1)} n^{2q+k-1} b_n = O(1).$$

It follows from (4.7) and consistency that either

$$R^{2q+k-1} S_R{}^{\delta+2q+\frac{1}{2}(k-1)}(h,0) = o(1) \tag{4.8}$$

as $R \to \infty$ or that for some sequence $\tau_1 < \tau_2 < \cdots < \tau_p \to \infty$,

$$R^{2q+k-1} S_R{}^{\tau_r+2q+\frac{1}{2}(k-1)}(h,0) \neq o(1) \qquad (r = 1, 2, \cdots) \tag{4.9}$$

as $R \to \infty$. However, since $g(t) = o(t^{2q})(C_k)$ as $t \to +0$ it follows from (4.6) (with δ replaced by τ), and arguments similar to those in the proof of Theorem 2, that for *some* τ_0 $R^{2q+k-1} S_R{}^{\tau+2q+\frac{1}{2}(k-1)}(h,0) = O(1)$ $(\tau \geqq \tau_0)$ i.e. that (4.9) is false. Hence (4.8) holds and so by (4.6) and Lemmas 4 and 5 $\sum n^q A_n(x^0)$ is summable $(n, \delta + 2q)$ to zero.

The case k even is proved in a similar way.

5. Supplementary remarks. Condition (ii) of Theorem 3 may be rephrased as "the $(2q + k - 1)$-th derived Fourier series of $h(t)$ is summable $(C, \delta + 2q + \frac{1}{2}k - \frac{1}{2})$ to $(2q + k - 1)!s$ at $t = 0$." Combining this observation with known results in the case $k = 1$ ([3] Theorem 2, [13] Lemma 2) we obtain the following result:

THEOREM 4. *If $\delta > \frac{1}{2}(k - 1)$, where k is an odd positive integer, then $(-)^q \sum n^q A_n(x^0)$ is summable $(n, \delta + 2q)$ to s if and only if there exist constants a_ν $(\nu = 0, \cdots, q - 1)$ such that* (i) *$t^{-2q-k+1}h(t)$ is integrable in the Cesaro-Lebesgue sense in $(0, \pi)$ and* (ii) *its Fourier cosine series is summable $(C, \delta - \frac{1}{2}k + \frac{1}{2})$ to s at $t = 0$.*

If they exist, the constants a_ν are given by (3.2).

For details of a similar calculation we refer to [13] Theorem 2.

It seems likely that the case k even of Theorem 3 can be reduced in a similar way, but the required one variable results are not known. On the other hand the imposition of additional conditions on $f(x)$ enables us to obtain various simplifications of Theorem 3 (case k even). We finally give a simple and useful result of this kind. Here we write $\omega(t)$ for the even periodic function which coincides with st^{2q+k-1} in $0 < t < \pi$. We also write

$$X(t) = h(t) - \omega(t) \tag{5.1}$$

and suppose

$$X(t) \sim \tfrac{1}{2}\gamma_0 + \sum \gamma_n \cos nt \tag{5.2}$$

$$\omega(t) \sim \tfrac{1}{2}\delta_0 + \sum \delta_n \cos nt. \tag{5.3}$$

We then have:

THEOREM 5. *If $\delta > \frac{1}{2}(k - 1)$ where k is an even integer and if there exist constants a_ν $(\nu = 0, \cdots, q - 1)$ such that $t^{-2q-k}X(t) \in L(0, \pi)$ then in order that $(-)^q \sum n^q A_n(x^0)$ be summable $(n, \delta + 2q)$ to s it is necessary and sufficient* (i) *that the $(2q + k - 1)$-th derived allied series of the even function $X(t)$ be summable $(C, \delta + 2q + \frac{1}{2}k - \frac{1}{2})$ at $t = 0$ or equivalently* (ii) *that the allied series of the odd periodic function equal to $t^{-2q-k+1}X(t)$ in $0 < t < \pi$, be summable $(C, \delta - \frac{1}{2}k + \frac{1}{2})$ at $t = 0$.*

If they exist the constants a_ν *are given by* (3.2).

Proof. It is easily verified that $t^{-2q-k}\chi(t) \in L(0, \pi)$ implies that

$$\int_0^t \chi(u)\,du = o(t^{2q+k})$$

as $t \to +0$, and hence, from (5.1), that $g(t) \sim st^{2q}(C_k, 1)$ as $t \to +0$. Consequently the initial assumption of Theorem 5 ensures that condition (i) of Theorem 3 is satisfied. Moreover a straightforward calculation shows that for $\delta > \frac{1}{2}(k-1)$ $n^{2q+k}\delta_n \to (-)^{\frac{1}{2}k+q}(2q+k-1)!2s/\pi\,(C, \delta+2q+\frac{1}{2}k+\frac{1}{2})$ so that from (5.1), (5.2), (5.3)

$$n^{2q+k}b_n \to (-)^{\frac{1}{2}k+q}(2q+k-1)!2s/\pi\,(C, \delta+2q+\frac{1}{2}k+\frac{1}{2})$$

if and only if

$$n^{2q+k}\gamma_n = O(1)\,(C, \delta+2q+\tfrac{1}{2}k+\tfrac{1}{2}) \tag{5.4}$$

as $n \to \infty$ i.e. condition (ii)′ of Theorem 3 is satisfied if and only if (5.4) holds.

Sufficiency of (i). Suppose that $\sum_{n=1}^{\infty} n^{2q+k-1}\gamma_n$ is summable $(C, \delta+2q+\frac{1}{2}k-\frac{1}{2})$ then $n^{2q+k}\gamma_n = o(1)$ $(C, \delta+2q+\frac{1}{2}k+\frac{1}{2})$ i.e. (5.4) holds so that condition (ii)′ of Theorem 3 is satisfied. Since condition (i) of that theorem is also satisfied it follows that $(-)^q \sum n^q A_n(x^0)$ is summable $(n, \delta+2q)$ to s.

Necessity of (i). Suppose that $(-)^q \sum n^q A_n(x^0)$ is summable $(n, \delta+2q)$ to s then condition (ii)′ of Theorem 3 is satisfied and hence (5.4) holds. Since $t^{-2q-k}\chi(t) \in L(0, \pi)$ it follows [3] that the $(2q+k-1)$-th derived allied series at $t = 0$ of $\chi(t)$ is summable (C) i.e. $\sum n^{2q+k-1}\gamma_n$ is summable (C). This together with (5.4) implies that $\sum n^{2q+k-1}\gamma_n$ is summable $(C, \delta, +2q+\frac{1}{2}k-\frac{1}{2})$.

The equivalence of conditions (i) and (ii) follows, in virtue of the integrability of $t^{-2q-k}\chi(t)$, from a result due to Bosanquet [3].

DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF ABERDEEN,
SCOTLAND.

REFERENCES.

[1] S. Bochner and K. Chandrasekharan, "Lattice points and Fourier expansions," *Acta Szeged*, vol. 12 (1950), pp. 1-15.

[2] S. Bochner, "Summation of multiple Fourier series by spherical means," *Transactions of the American Mathematical Society*, vol. 40 (1936), pp. 175-207.

[3] L. S. Bosanquet, "The Cesaro summability of the successively derived allied series of a Fourier series," *Proceedings of the London Mathematical Society*, (2) vol. 49 (1945), pp. 63-77.

[4] ———, "A solution of the Cesaro summability problem for successively derived Fourier series," *Proceedings of the London Mathematical Society*, (2) vol. 46 (1940), pp. 270-289.

[5] K. Chandrasekharan, "On the summation of multiple Fourier series I," *Proceedings of the London Mathematical Society*, (2) vol. 50 (1948), pp. 210-222.

[6] ———, "On Fourier series in several variables," *Annals of Mathematics*, vol. 49 (1948), pp. 991-1007.

[7] ——— and S. Minakshisundaram, *Typical Means* (1952).

[8] G. H. Hardy, "The second theorem of consistency for summable series," *Proceedings of the London Mathematical Society*, (2) vol. 15 (1916), pp. 72-88.

[9] V. L. Shapiro, "The circular summability of trigonometric series," *Transactions of the American Mathematical Society*, vol. 76 (1954), pp. 223-233.

[10] ———, "Generalized Laplacians of the second kind and double trigonometric series," *Duke Mathematical Journal*, vol. 21 (1954), pp. 173-178.

[11] G. N. Watson, *A treatise on Bessel Functions* (1922).

[12] S. Verblunsky, "Note on the sum of an oscillating series," *Proceedings of the Cambridge Philosophical Society*, vol. 26 (1930), pp. 152-157.

[13] A. J. White, "On the summability, by spherical Riesz means, of multiple Fourier series," *Journal of the London Mathematical Society*, vol. 35 (1960), pp. 495-502.

[14] A. Zygmund, *Trigonometric Series II*, Cambridge, 1959.

THE COHOMOLOGY OF DIFFERENTIABLE TRANSFORMATION GROUPS.* [1]

By RICHARD S. PALAIS and THOMAS E. STEWART.

1. Introduction. If a Lie group G acts differentiably on a manifold $\mathfrak{M}$ then various spaces of tensor field on $\mathfrak{M}$ become in a natural way modules for the Lie algebra $\mathfrak{g}$ of G and the cohomology of $\mathfrak{g}$ with these coefficient modules in certain cases carries interesting information about the action of G. In this paper we will discuss this situation, at first in a somewhat more abstract setup, and develop a method for computing these cohomology groups in certain cases. In particular we shall show that if G is compact and semi-simple then even though these modules are infinite dimensional the conclusions of the First and Second Whitehead Lemmas [10], [11] are valid; namely the first and second cohomology groups are trivial. As one consequence we will show that differentiable actions of compact, semi-simple Lie groups admit only trivial infinitesimal deformations (§ 11) a fact whose global analogue will be found in [7]. Our second and motivating application of these general cohomology results is to a question initiated by one of the authors in [9]. Namely if a Lie group G acts differentiably on the base space of a differentiable fiber bundle B over M can G be made to act differentiably on B so as to be equivariant with respect to the fiber projection and so that each operation of G on B is a bundle map. We show here that the answer is yes if G is compact and simply connected and if the structural group of B is a solvable Lie group, and moreover that the way of "lifting" the action of G to B is essentially unique.

2. Cohomology and invariant cohomology of Lie algebras. In the following L is a finite dimensional Lie algebra over a field F of characteristic zero. For the defintion of an L-module and a complete discussion of the cohomology of L with coefficients in an L-module we refer the reader to [2] or [3] (we shall use the notation of the latter). The notion of the invariant cohomology of L with coefficients in an L-module is implicit in a number of

---

* Received February 27, 1961.

[1] This research has been carried out in part under the sponsorship of the National Science Foundation (Grant No. 614227) and the Army Research Office (Durham).

papers, however the lack of an exposition with the relevant facts that we shall need makes the following discussion desirable.

Recall that if M is an L-module then the space $C^p(L,M)$ of p-cochains of L with coefficients in M is defined to be M if $p=0$ and to be the space of alternating multilinear maps of L^p into M if p is a positive integer. Then $C^*(L,M)$ the cochain complex of L with coefficients in M is the graded vector space $\bigoplus_{p\geqq 0} C^p(L,M)$ with the differential d of degree $+1$ defined by $dm(X)=X\cdot m$ for $m\in M$ and

$$(1)\qquad \begin{aligned} dc(X_1,\cdots,X_{p+1}) &= \sum_{i=1}^{p+1}(-1)^{i+1}X_i(c(X_1,\cdots,\hat{X}_i,\cdots,X_{p+1})) \\ &\quad + \sum_{i<j}(-1)^{i+j}c([X_i,X_j],X_1,\cdots,\hat{X}_i,\cdots,\hat{X}_j,\cdots,X_{p+1}) \end{aligned}$$

for $c\in C^p(L,M)$, $p>0$. We recall from [3] that $d^2=0$ so there are defined graded vector spaces $Z^*(L,M)$ and $B^*(L,M)$ of cocycles and coboundaries and their quotient $H^*(L,M)$ the cohomology space of L with coefficients in M. We recall also that $C^*(L,M)$ becomes a graded L-module with $M=C^0(L,M)$ as a submodule if we define

$$(2)\qquad \begin{aligned} (Xc)(X_1,\cdots,X_p) &= X(c(X_1,\cdots,X_p)) - \sum_{i=1}^{q} c(X_1,\cdots,[X,X_i],\cdots X_p) \\ &= X(c(X_1,\cdots,X_p)) - \sum_{i=1}^{q}(-1)^{i+1}c([X,X_i],X_1,\cdots,\hat{X}_i,\cdots X_p) \end{aligned}$$

for $c\in C^p(L,M)$, $p>0$, and that

$$(3)\qquad d(Xc)=X(dc)$$

for $X\in L$, $c\in C^*(L,M)$. It follows from (1) and (2) that for $c\in C^p(L,M)$

$$\begin{aligned} dc(X_1,\cdots,X_{p+1}) &= \sum_{i=1}^{p+1}(-1)^{i+1}(X_ic)(X_1,\cdots,\hat{X}_i,\cdots X_{p+1}) \\ &\quad + \sum_{i<j}(-1)^{i+j+1}c([X_i,X_j],X_1,\cdots,\hat{X}_i,\cdots\hat{X}_j,\cdots X_{p+1}) \end{aligned}$$

We define a cochain $c\in C^*(L,M)$ to be *invariant* if $Xc=0$ for all $X\in L$. It follows from (3) that the graded subspace $C_I^*(L,M)=\bigoplus_{p\geqq 0} C_I^p(L,M)$ of $C^*(L,M)$ consisting of invariant cochains is stable under d and so gives rise to the graded vector spaces $Z_I^*(L,M)$ and $B_I^*(L,M)$ of invariant cocycles and invariant coboundaries (N.B. $B_I^*(L,M)=dC_I^*(L,M)$ *not* the possibly larger $C_I^*(L,M)\cap B^*(L,M)$) and their quotient $H_I^*(L,M)$ which we call the *invariant cohomology* of L with coefficients in M. By the *natural homomorphism* of $H_I^*(L,M)$ into $H^*(L,M)$ we mean the homomorphism induced by the inclusion of $C_I{}^*(L, M)$ in $C^*(L, M)$. We note from (4) that $d_I = d | C_I{}^*(L, M)$ is given on $C^p(L, M)$ by

$$(5) \quad d_I c(X_1, \cdots, X_{p+1}) = -\sum_{i<j} (-1)^{i+j} c([X_i, X_j], X_1, \cdots X_i, \cdots X_j, \cdots X_{p+1})$$

An L-module M is called *trivial* if $Xm = 0$ for all $X \in L$, $m \in M$ (i.e. if $C_I{}^0(L, M) = C^0(L, M) = M$). Any vector space V over F can be considered a trivial L-module, in which case we write d_T for the differential on $C^*(L, V)$. Clearly from (1)

$$(6) \quad d_T c(X_1, \cdots, X_p) = \sum_{i<j} (-1)^{i+j} c([X_i, X_j], X_1, \cdots X_i \cdots X_j, \cdots X_{p+1}).$$

In particular we regard F as a trivial L-module and write $C^*(L, F) = C^*(L)$ and $H^*(L, F) = H^*(L)$. Since $C^1(L) = L^*$, the dual space of L, and since by (6) $d_T c(X, Y) = c([X, Y])$ for $c \in C^1(L)$ it follows that $Z^1(L) = [L, L]^0$, the annihilator of $[L, L]$. Since $B^1(L)$ is clearly zero (for $df(X) = 0$ for $f \in F$) it follows that $H^1(1) \cong Z^1(L) = [L, L]^0 \cong (L/[L, L])^*$. Thus $H^1(L)$ is trivial if and only if L is its own commutator subalgebra. Note also that H^* is an additive functor, i.e. $H^*(L, M \oplus N) \cong H^*(L, M) \oplus H^*(L, N)$, so it follows that if $H^p(L) = 0$ then $H^p(L, V) = 0$ for any trivial finite dimensional L-module V.

If M is any L-module then for each $X \in L$ there is an endomorphism i_X of $C^*(L, M)$ homogeneous of degree -1 defined by $i_X m = 0$ for $m \in M = C^0(L, M)$ and $(i_X c)(X_1, \cdots, X_{p-1}) = c(X, X_1, \cdots, X_{p-1})$ for $c \in C^p(L, M)$, $p > 0$. For later reference we recall from [3] that the module operations of L on $C^*(L, M)$ is related to d and the operations i_X by

$$(7) \qquad Xc = d i_X c + i_X dc \qquad X \in L, c \in C^*(L, M).$$

3. An extension of the Whitehead lemmas. We will show in § 8 that if $\mathfrak{G}$ is the Lie algebra of a compact Lie group then for a certain class of $\mathfrak{G}$-modules M the natural homomorphism of $H_I{}^*(\mathfrak{G}, M)$ into $H^*(\mathfrak{G}, M)$ is an isomorphism onto. If $\mathfrak{G}$ is semi-simple it follows from the theorems we are above to prove that for such $\mathfrak{G}$-modules $H^1(\mathfrak{G}, M)$ and $H^2(\mathfrak{G}, M)$ are trivial, a fact that would also be a consequence of the Whitehead Lemmas ([10] and [11]) if M were finite dimensional. It is in this sense that this theorem extends the Whitehead lemmas.

THEOREM. *If L is a finite dimensional Lie algebra such that $H^1(L) = 0$ then $H_I{}^1(L, M) = 0$ for all L-modules M. If in addition $H^2(L) = 0$ then $H_I{}^2(L, M) = 0$ for all L-modules M.*

Proof. $C_I{}^0(L,M) = \{m \in M \mid Xm = 0 \text{ for all } X \in L\}$ so if $m \in C_I{}^0(L,M)$ then $dm(X) = Xm = 0$ for all $X \in L$ hence $B_I{}^1(L,M) = 0$ and $H_I{}^1(L,M) \cong Z_I{}^1(L,M)$. By (5) of § 2 if $c \in C_I{}^1(L,M)$ then $dc(X,Y) = c([X,Y])$ so $Z_I{}^1(L,M) = \{c \in C_I{}^1(L,M) \mid c \text{ is zero on } [L,L]\}$. But $H^1(L) = 0$ is equivalent to $L = [L,L]$ and hence implies $H_I{}^1(L,M) \cong Z_I{}^1(L,M) = 0$.

Now let $c \in Z_I{}^2(L,M)$ and let V be the finite dimensional subspace of M spanned by $\{c(X,Y) \mid X,Y \in L\}$. We consider V as a trivial L-module. Assuming $H^2(L) = 0$ it follows that $H^2(L,V) = 0$. Now $c \in C^2(L,V)$ and comparing (5) and (6) of § 2 we see that $d_T c = - d_I c = 0$ so $c \in Z^2(L,V) = B^2(L,V)$ and hence $C = d_T\theta$ for some $\theta \in C^1(L,V) \subset C^1(L,M)$. It will suffice to prove that $\theta \in C_I{}^1(L,M)$, for then comparing (5) and (6) of § 2 again, $d_I(-\theta) = -d_I\theta = d_T\theta = c$ so $c \in B_I{}^2(L,M)$ and we will have shown $Z_I{}^2(L,M) = B_I{}^2(L,M)$. Now if $X, X_1, X_2 \in L$ then from (2) of § 2

$$0 = (Xc)(X_1,X_2) - X(c(X_1,X_2)) - c([X,X_1],X_2) - c(X_1,[X,X_2])$$

$$= X(\theta([X_1,X_2])) - \theta([[X,X_1],X_2]) - \theta([X_1,[X,X_2]])$$

and by the Jacobi identity and the linearity of θ it follows that

$$0 = X(\theta([X_1,X_2])) - \theta([X,[X_1,X_2]])$$

so, referring to (2) of § 2 again, $(X\theta)([X_1,X_2]) = 0$. Thus $X\theta$ vanishes on $[L,L] = L$ so θ is invariant. q. e. d.

4. Topological G-Modules.

In this and succeeding sections G will denote a compact Lie group, G_0 its identity component, and $\mathfrak{G}$ its Lie algebra of left invariant vector fields. By a *topological G-module* we shall mean a complete, metrizable, locally convex, real topological vector space (a Frechét space) M together with a fixed homomorphism T of G into the group of automorphisms of M such that for each $m \in M$ the map $g \to T(g)m$ of G into M is continuous. We denote the space of continuous linear functionals on M by M^* and we write $\langle m,l \rangle$ for $l(m)$ if $(l,m) \in M^* \times M$ (which of the many possible topologies to put on M^* is irrelevant for our purposes and we shall always regard M^* as untopologized). In general we will drop explicit reference to T and simply write gm instead of $T(g)m$. Note that since M is a Frechét space and for each $m \in M$ the orbit $\{gm \mid g \in G\}$ is compact, and hence bounded, it follows from the principle of uniform boundedness that

4.1. THEOREM. *Given a neighborhood V of zero in the topological G-module M there is a neighborhood U of zero in M such that $gu \in V$ for all $(g,u) \in G \times U$. Equivalently if $\{m_r\}$ is a sequence in M converging to m then $\{gm_r\}$ converges to gm uniformly for $g \in G$.*

Noting that $g_r m_r - gm = g_r(m_r - m) + (g_r m - gm)$ it follows from 4.1 that if $g_r \to g$ then $g_r m_r \to gm$.

4. 2. COROLLARY. *If M is a topological G module then $(g, m) \to gm$ is a continuous map of $G \times M$ into M.*

Now let M be a topological G-module and M^X the linear space of functions from a compact Hausdorff space X into M. We give M^X the topology of uniform convergence, i. e. a typical neighborhood of zero is $\{f \in M^X \mid f(X) \subseteq U\}$ where U is some neighborhood of zero in M. By a step function from X to M we mean an element $f \in M^X$ whose range is a finite subset $\{m_1, \cdots, m_r\}$ of M such that each $f^{-1}(m_i)$ is Borel measurable. Since a continuous function from X to M is uniformly continuous it follows easily that the space $C(X, M)$ of continuous maps of X to M is included in the closure of the space $S(X, M)$ of step functions. Given a Radon measure μ on X and $f \in S(X, M)$ we define $\int f d\mu = \sum_{m \in M} \mu(f^{-1}(m))m$. Then $f \to \int f d\mu$ is a continuous linear map from $S(X, M)$ into M and so (because M is complete) extends to a continuous linear map of the closure of $S(X, M)$ into M. Henceforth we shall only be concerned with $\int f d\mu$ when f is continuous and we shall need the following obvious facts.

(a) $f_\alpha \to f$ uniformly on $X \Rightarrow \int f_\alpha d\mu \to \int f d\mu$

(b) $\int f d\mu$ is bilinear in f and μ

(c) If $\mu(X) = 1$ then $\int f d\mu \in$ closed convex hull of $f(X)$.

(d) If T is a continuous linear map of M into a complete topological vector space then $\int (Tf) d\mu = T \int f d\mu$.

The space $C(G)$ of continuous real valued functions on G is a Banach space in the supremum norm and becomes a topological G-module under the operations given by $(gf)(x) = f(g^{-1}x)$. If $f \in C(G)$ we define $f * m$, for m an element of a topological G-module M, to be the integral of the continuous map $g \to f(g)gm$ of G into M with respect to normalized Haar measure on G. If $l \in M^*$ then by (d) above $\langle f * m, l \rangle = \int f(g) \langle gm, l \rangle d \cdot g$. From this and the invariance of Haar measure it follows that $\langle (gf) * m, l \rangle = \langle g(f * m), l \rangle$ and since M^* separates points of M it follows that $(gf) * m = g(f * m)$.

4. 3. THEOREM. *If M is a topological G-module then*

(1) *$(f, m) \to f * m$ is a continuous bilinear map of $C(G) \times M$ into M*

(2) *If $f \in C(G)$ is positive and $\int f(g) dg = 1$ then $f * m \in$ closed convex hull of $\{gm \mid f(g) \neq 0\}$.*

(3) *If $m \in M$ then $f \to f * m$ is an equivariant continuous linear map of $C(G)$ into M and m is in the closure of its range.*

Proof. Statement (1) is immediate from (a) and (b) above and state-(2) follows from (c). The equivariance of $f \to f * m$ (i.e. the fact that $(gf) * m = g(f * m)$ was shown above so it remains only to show that if W is a closed convex neighborhood of m in M then there is an $f \in C(G)$ such that $f * m \in W$. Let U be a neighborhood of the identity in G such that $gm \in W$ for $g \in U$ and let f be a continuous positive function of integral one on G with support in U. Then by (2) $f * m \in W$. q.e.d.

5. Almost invariant vectors. An element m_0 of a topological G-module M is called *almost invariant* if $\{gm_0 | g \in G\}$ spans a finite dimensional subspace of M. We denote the set of almost invariant vectors in M by M_0. Clearly M_0 is a subspace of M invariant under G, and in fact M_0 is just the linear span of the finite limensional G-invariant subspaces of M. An almost invariant vector in $C(G)$ is called an almost invariant function on G. From the bilinearity of $(f, m) \to f * m$ and the equivariance of $f \to f * m$ it follows that if f_0 is an almost invariant function and m any element of a topological G-module M then $f_0 * m \in M_0$. Now the Peter-Weyl theorem [1, p. 203] says that the almost invariant functions are dense in $C(G)$. Since we known that m is adherent to $\{f * m | f \in C(G)\}$ and that $f \to f * m$ is continuous we have the following essentially known result.

5.1. THEOREM. *In any topological G-module M the subspace M_0 of almost invariant vectors is dense.*

5.2. THEOREM. *If M is any topological G-module then the subspace M_0 of almost invariant vectors has a $\mathfrak{g}$-module stducture defined by $Xm = \lim_{t \to 0} 1/t((\operatorname{Exp} tX)m - m)$ for $X \in \mathfrak{g}$, $m \in M_0$.*

Proof. If V is any finite dimensional invariant subspace of M_0 $(g, v) \to gv$ is an analytic map of $G \times V \to V$ (this follows for example from [1, Prop 1, p. 128]) so that the indicated limit exists for $m \in V$. That this gives a $\mathfrak{g}$-module on V follows from [1, Theorem 2, p. 113]. Since M_0 is the linear span of its finite dimensional invariant subspaces the theorem follows.

q.e.d.

6. Differentiable G-modules.

6.1. LEMMA. *Let M be a topological G-module and $\{m_r\}$ a sequence in M converging to m. Given $X \in \mathfrak{g}$ and $l \in M^*$ suppose there exists a sequence*

$\{\omega_k\}$ in M converging to ω such that $d/dt\langle(\mathrm{Exp}\, tX)m_r, l\rangle = \langle(\mathrm{Exp}\, tX)\omega_r, l\rangle$. Then $d/dt\langle(\mathrm{Exp}\, tX)m, l\rangle = \langle(\mathrm{Exp}\, tX)\omega, l\rangle$.

Proof. By 4.1 gm_r converges to gm uniformly in g, so since l is linear and continuous and hence uniformly continuous, $\langle gm_r, l\rangle$ converges to $\langle gm, l\rangle$ uniformly in g and *a fortiori* $\langle(\mathrm{Exp}\, tX)m_k, l\rangle$ converges to $\langle(\mathrm{Exp}\, tX)m, l\rangle$ uniformly in t. Similarly $\langle(\mathrm{Exp}\, tX)\omega_k, l\rangle$ converges to $\langle(\mathrm{Exp}\, tX)\omega, l\rangle$ uniformly in t. By a theorem of elementary calculus this validates differentiation "under the limit sign" and gives the desired result. q. e. d.

6.2. THEOREM. *Let M be a topological G-module $X \in \mathfrak{G}$, and suppose there is a function $\bar{X}: M \to M$ such that*

$$d/dt\langle(\mathrm{Exp}\, tX)m, l\rangle = \langle(\mathrm{Exp}\, tX)\bar{X}m, l\rangle$$

for all $m \in M$ and all l belonging to a separating family $S \subset M^*$. Then $\bar{X}$ is a continuous linear map and for $m \in M_0$ $Xm = \lim_{t\to 0} 1/t((\mathrm{Exp}\, TX)m - m)$.

Proof. The linearity of $\bar{X}$ is immediate from the linearity of differentiation and the fact that S is separating. The preceding lemma gives immediately that $\bar{X}$ has a closed graph and, since M is a Frechét space $\bar{X}$ is continuous. If $m \in M_0$ then by 5.2 $1/t((\mathrm{Exp}\, tX)m - m)$ converges strongly and *a fortiori*, weakly to a limit say m'. By definition of $\bar{X}$ $\langle m', l\rangle = \langle\bar{X}m, l\rangle$ for $l \in S$ and again since S is separating $m' = \bar{X}m$. q. e. d.

6.3. THEOREM. *Let M be a topological G-module, $X \in \mathfrak{G}$, and suppose that the linear map*

$$m \to \lim_{t\to 0} 1/t((\mathrm{Exp}\, tX)m - m)$$

of M_0 into itself (see 5.2) *is continuous. Then this map extends uniquely to a continuous linear map $\bar{X}$ of M into itself and $d/dt\langle(\mathrm{Exp}\, tX)m, l\rangle = \langle(\mathrm{Exp}\, tX)\bar{X}m, l\rangle$ for all $m \in M$, $l \in M^*$.*

Proof. The existence and uniqueness of $\bar{X}$ follows from the completeness of M and the denseness of M_0 in M. Given $l \in M^*$, $m \in M_0$, and t_0 a real number $l_0: m \to \langle(\mathrm{Exp}\, t_0X)m, l\rangle$ is an element of M^* and

$$\begin{aligned}\frac{d}{dt}\Big|_{t=t_0}\langle(\mathrm{Exp}\, tX)m_0, l\rangle &= \frac{d}{dt}\Big|_{t=0}\langle(\mathrm{Exp}(t+t_0)X)m_0, l\rangle \\ &\frac{d}{dt}\Big|_{t=0}\langle(\mathrm{Exp}\, tX)m_0, l_0\rangle = \langle\bar{X}m_0, l_0\rangle = \langle(\mathrm{Exp}\, t_0X)\bar{X}m_0, l\rangle.\end{aligned}$$

Thus $\langle(\mathrm{Exp}\, tX)m, l\rangle$ is differentiable for $m \in M_0$ and $l \in M^*$ and its derivative is $\langle(\mathrm{Exp}\, tX)\bar{X}m, l\rangle$. If m is an arbitrary element of M choose a sequence $\{m_r\}$ in M_0 converging to m. Then $\bar{X}m_r \to \bar{X}m$ and for any $l \in M^*$

$d/dt\langle(\operatorname{Exp} tX)m_r, l\rangle = \langle(\operatorname{Exp} tX)\tilde{X}m_r, l\rangle$ so by 6.1 $d/dt\langle(\operatorname{Exp} tX)m, l\rangle = \langle(\operatorname{Exp} tX)\tilde{X}m, l\rangle$. q. e. d.

6.4. THEOREM. *If M is a topological G-module then the following are equivalent conditions.*

(1) *For each $X \in \mathfrak{G}$ there is a function $\tilde{X}: M \to M$ such that for all l in a separating subset of M^* $\frac{d}{dt}\langle(\operatorname{Exp} tX)m, l\rangle = \langle(\operatorname{Exp} tX)Xm, l\rangle$ for all $m \in M$.*

(2) *For each $X \in \mathfrak{G}$ the map $X^0: m \to \lim_{t\to 0} 1/t((\operatorname{Exp} tX)m - m)$ of M_0 into itself* (see 5.2) *is continuous.*

(3) *For each $X \in \mathfrak{G}$ and $m \in M$ $t \to (\operatorname{Exp} tX)m$ has a weak derivative, X'_m, at $t = 0$.*

(4) *For each $X \in \mathfrak{G}$ there is a map $X^*: M \to M$ such that*

$$\frac{d}{dt}\langle(\operatorname{Exp} tX)m, l\rangle = \langle(\operatorname{Exp} tX)X^*m, l\rangle.$$

Moreover if any one, and hence all, of these conditions are satisfied then the maps X, X', and X^* are all equal and are the unique continuous linear map of M into intself which extends X^0.

Proof. It is clear that (4) implies (1) and that if $\tilde{X}$ and X^* exist that they are equal. From 6.2 it follows that (1) implies (2) and that if $\tilde{X}$ exists, it is the unique continuous linear extension of X^0. From 6.3 it follows that (2) implies (3) and that X^* is the unique continuous linear extension of X^0. It remains to show that (3) implies (4) and that $X' = X^*$. Assuming (3) holds let $l \in M^*$ and t_0 a real number and define $l_0 \in M^*$ by $m \to \langle(\operatorname{Exp} t_0X)m, l\rangle$. Then for any $m \in M$

$$\left.\frac{d}{dt}\right|_{t=t_0}\langle(\operatorname{Exp} tX)m, l\rangle = \left.\frac{d}{dt}\right|_{t=0}\langle(\operatorname{Exp}((t+t_0)X)m, l\rangle$$

$$\left.\frac{d}{dt}\right|_{t=0}\langle(\operatorname{Exp} tX)m, l_0\rangle = \langle X'm, l_0\rangle = \langle(\operatorname{Exp} t_0X)X'm, l\rangle.$$

This shows both that (4) holds and that $X^*m \equiv X'm$.

q. e. d.

6.5. *Definition.* A topological G-module is called differentiable if it satisfies any one and hence all of the properties (1)-(4) of 6.4.

Remark. It is easily shown by example that the maps $t \to (\operatorname{Exp} tX)m$ need not be strongly differentiable for all m in a differentiable G-module.

6.6. THEOREM. *If M is a differentiable G-module then M has a $\mathfrak{G}$-module structure which is characterized by the identity*

$$\langle Xm, l\rangle = \frac{d}{dt}\bigg|_{t=0}\langle (\operatorname{Exp} tX)m, l\rangle$$

for $X \in \mathfrak{G}$, $m \in M$, $l \in M^*$. Moreover each of the module operations of $\mathfrak{G}$ on M is continuous.

Proof. Immediate from 5.1, 5.2, and 6.4.

6.7. *Definition.* If M is a differentiable G-module then the $\mathfrak{G}$-module structure for M described in 6.6 is called the derived $\mathfrak{G}$-module.

Henceforth differentiable G-modules will be regarded without explicit mention as $\mathfrak{G}$-modules, the derived $\mathfrak{G}$-module always being understood.

6.8. THEOREM. *If M is a differentiable G-module then:*

(1) $\dfrac{d}{dt}\langle (\operatorname{Exp} tX)m, l\rangle = \langle (\operatorname{Exp} tX)Xm, l\rangle X \in \mathfrak{G}$, $m \in M$, $l \in M^*$

(2) $gXg^{-1}m = (ad(g)X)m$, $X \in \mathfrak{G}$, $g \in G$, $m \in M$

(3) *If $m \in M$ then $Xm = 0$ for all $X \in \mathfrak{G}$ if and only if $gm = m$ for all $g \in G_0$.*

Proof. (1) follows easily from 6.4 and the definition of the derived $\mathfrak{G}$ module structure. To prove (2) we note that if $l \in M^*$ and we write $\bar{l} = l \circ g$ then

$$\begin{aligned}\langle (ad(g)X)m, l\rangle &= \frac{d}{dt}\bigg|_{t=0}\langle \operatorname{Exp} t(ad(g)X)m, l\rangle \\ &= \frac{d}{dt}\bigg|_{t=0}\langle g(\operatorname{Exp} tX)g^{-1}m, l\rangle \\ &= \frac{d}{dt}\bigg|_{t=0}\langle (\operatorname{Exp} tX)(g^{-1}m), \bar{l}\rangle \\ &= \langle Xg^{-1}m, \bar{l}\rangle = \langle gXg^{-1}m, l\rangle.\end{aligned}$$

If $gm = m$ for all $g \in G_0$ then $(\operatorname{Exp} tX)m = m$ for all $X \in \mathfrak{G}$ and all real t hence for each $X \in \mathfrak{G}$ $t \to (\operatorname{Exp} tX)$ has strong and therefore weak derivative zero at $t = 0$ and by Definition $Xm = 0$. Conversely if $Xm = 0$ for a given $X \in \mathfrak{G}$ then by (1) $\dfrac{d}{dt}\langle \operatorname{Exp} tX, l\rangle \equiv 0$ so $\langle (\operatorname{Exp} tX)m, l\rangle \equiv \langle (\operatorname{Exp} 0X)m, l\rangle = \langle m, l\rangle$, $(\operatorname{Exp} tX)m \equiv m$. Since G is compact every element of G_0 is of the form $\operatorname{Exp} X$ and (3) follows. q. e. d.

7. The differentiable structure of $C^*(\mathfrak{g}, M)$. In this section we will show that if M is a differentiable G-module then $C^*(\mathfrak{g}, M)$ is in a natural way a differentiable G-module also. Moreover we shall show that the derived $\mathfrak{g}$-module structure for $C^*(\mathfrak{g}, M)$ coincides with the other "natural" $\mathfrak{g}$-module structure that it has *qua* cochain complex of the $\mathfrak{g}$-module M (§ 1, equation (2)). Finally we shall show that the differential d is continuous on $C^*(\mathfrak{g}, M)$ and commutes with each operation of G.

Since $C^*(\mathfrak{g}, M) = \bigoplus\limits_p C^p(\mathfrak{g}, M)$ and $C^p(\mathfrak{g}, M) = 0$ for $p > \dim \mathfrak{g}$, to define a differentiable G-module structure on $C^*(\mathfrak{g}, M)$ it suffices to define one on each $C^p(\mathfrak{g}, M)$, $p > 0$. For a typical neighborhood of zero in $C^p(\mathfrak{g}, M)$ we take $\{c \in C^p(\mathfrak{g}, M) \mid c(X_1, \cdots, X_p) \in U \text{ if } X_1, \cdots, X_p \in B\}$ where B is a compact subset of $\mathfrak{g}$ and U a neighborhood of zero in M. Thus $c_\alpha \to c$ means that for each compact subset B of M c_α converges uniformly to c on B^p. The metrizeability, completeness, and local convexity of $C^p(\mathfrak{g}, M)$ follow directly from the corresponding properties of M. The operations of G on $C^p(\mathfrak{g}, M)$ are defined by $(gc)(X_1, \cdots, X_p) = g(c(ad(g^{-1})X_1, \cdots, ad(g^{-1})X_p))$. It is obvious that each such operation is an automorphism of $C^p(\mathfrak{g}, M)$ and that $(g_1 g_2)c = g_1(g_2 c)$. That $g \to gc$ is a continuous map of G into $C^p(\mathfrak{g}, M)$ for any $c \in C^p(\mathfrak{g}, M)$ is a straightforward argument which we leave to the reader. Given $X_1, \cdots, X_p$ in $\mathfrak{g}$ and a $l \in M^* c \to \langle c(X_1, \cdots, X_p), l \rangle$ is an element of $C^p(\mathfrak{g}, M))^*$ and the collection of such continuous linear functionals on $C^p(\mathfrak{g}, M)$ is clearly separating. Now put

$$g(t) = c(ad(\operatorname{Exp} - tX)X_1, \cdots, ad(\operatorname{Exp} - tX)X_p).$$

From the well-known fact that

$$\lim_{t \to t_0} \frac{1}{t - t_0} (ad(\operatorname{Exp} tX)Y - ad(\operatorname{Exp} t_0 X)Y) = ad(\operatorname{Exp} t_0 X)[X, Y]$$

it follows from the multilinearity of c that $g(t)$ is strongly differentiable at t_0 and that

$$g'(t_0) = -\sum_{i=1}^{p} c(ad(\operatorname{Exp} - t_0 X)X_1, \cdots, ad(\operatorname{Exp} - t_0 X)[X, X_i], \\ \cdots, ad(\operatorname{Exp} - t_0 X)X_p).$$

(We have used the fact that a multilinear map of a finite dimensional space into a topological vector space is automatically continuous.) Putting $\lambda(t) = (\operatorname{Exp} tX)g(t)$ we have

$$\frac{1}{1 - t_0}(\lambda(t) - \lambda(t)) = \frac{1}{t - t_0}((\operatorname{Exp} tX)g(t_0) - g(t_0)) \\ + (\operatorname{Exp} tX)(\frac{1}{t - t_0}(g(t) - g(t_0))$$

By the joint continuity of $G \times C^p(\mathfrak{g}, M) \to C^p(\mathfrak{g}, M)$ the second term converges to $(\operatorname{Exp} t_0X)g'(t_0)$ as t converges to t_0 while by (1) of 6.8 the first term converges weakly to $(\operatorname{Exp} t_0X)Xg(0)$. Thus if $l \in M^*$ then

$$\begin{aligned}\frac{d}{dt}\Big|_{t=t_0}\langle((\operatorname{Exp} tX)c)(X_1,\cdots,X_p),l\rangle &= \frac{d}{dt}\Big|_{t=t_0}\langle\lambda(t),l\rangle \\ &= \langle((\operatorname{Exp} t_0X)(Xc))(X_1,\cdots,X_p),l\rangle\end{aligned}$$

where $Xc \in C^p(\mathfrak{g}, M)$ is defined in (2) of § 1. It follows that condition (1) of 6.2 is satisfied by the topological G-module $C^p(\mathfrak{g}, M)$ and hence that $C^p(\mathfrak{g}, M)$ is a differentiable G-module, the derived $\mathfrak{g}$-module structure moreover being that given in (2) of § 1. If $\{c_n\}$ is a sequence in $C^p(\mathfrak{g}, M)$ converging to c then it is clear from (1) of § 1 that for any $X_1,\cdots,X_{p+1}$ $dc_\alpha(X_1,\cdots,X_{p+1})$ converges in M to $dc(X_1,\cdots,X_p)$, from which it is clear that the map $d\colon C^p(\mathfrak{g}, M) \to C^{p+1}(\mathfrak{g}, M)$ has a closed graph and so, the domain and range being Frechét spaces, d is continuous. A similar argument shows that for each $X \in \mathfrak{g}$ the linear map $i_X\colon C^p(\mathfrak{g}, M) \to C^{p-1}(\mathfrak{g}, M)$ is continuous.

From (2) of (6.8) it follows that $Xgc = g(ad(g^{-1})X)$ for all $g \in G$, $X \in \mathfrak{g}$ and $c \in C^*(\mathfrak{g}, M)$. Using this and equation (1) of § 1 a straightforward computation gives $g(dc) = d(gc)$.

8. The main theorem.

8.1. Lemma. *If M is a differentiable G-module then each operation of G_0 on $C^*(\mathfrak{g}, M)$ is chain homotopic to the identity, i.e. for each $g \in G_0$ there is a linear map $\lambda(g)$ of $C^*(\mathfrak{g}, M)$ into itself such $gc - c = d\lambda(g)c + \lambda(g)dc$ for all $c \in C^*(\mathfrak{g}, M)$. Moreover, the map $g \to \lambda(g)$ can be cosen so that $g \to \lambda(g)c$ is continuous for each $c \in C^*(\mathfrak{g}, M)$.*

Proof. Since G_0 is compact and connected we can find, for each $g \in G_0$, $X \in \mathfrak{g}$ such that $g = \exp X$. We define $\lambda(g)\cdot c = \int_0^1 (\operatorname{Exp} tX)i_Xc\cdot dt$. Since $C^*(\mathfrak{g}, M)$ is a differentiable G-module from 6.8, (1) for any $l \in (C^*(\mathfrak{g}, M))^*$

$$\begin{aligned}\langle gc - c, l\rangle &= \int_0^1 \frac{d}{dt}\langle(\operatorname{Exp} tX)c, l\rangle dt \\ &= \int_0^1 \langle(\operatorname{Exp} tX)Xc, l\rangle dt \\ &= \langle\int_0^1 ((\operatorname{Exp} tX)Xc\, dt), l\rangle\end{aligned}$$

and recalling that $Xc = di_X c + i_X dc$ (§1, (7))

$$\langle gc - c, l\rangle = \langle \int_0^1 (\operatorname{Exp} tX)\, di_X c + \lambda(g)\, dc, l\rangle.$$

Since d commutes with $\operatorname{Exp} tX$ and integration we obtain

$$\langle gc - c, l\rangle = \langle d\lambda(g)c + \lambda(g)\, dc, l\rangle$$

This equation holds for all $l \in (C^*(\mathfrak{G}, M))^*$ and hence $\lambda(g)$ is a chain homotopy.

Now suppose that U is a small enough neighborhood of the identity so that the exponential map has a continuous inverse, f. Define then

$$\lambda_0(g)c = \int_0^1 (\operatorname{Exp} tf(g))\, i_{f(g)} c\, dt.$$

$\lambda_0(g)$ has the required properties and $g \to \lambda_0(g)c$ is continuous on U. Now choose $g_1, \cdots, g_n$ in G_0 so that $g_i U$ cover G_0, and choose $\lambda(g_i)$ satisfying the lemma. It is easily seen that if we define $\lambda_i(g)$ for $g = g_i u \in g_i U$ by

$$\lambda_i(g) = \lambda(g_i) + \lambda_0(u) + \lambda(g_i)\, d\lambda_0(u) + d\lambda(g_0)\lambda_0(u)$$

then $gc - c = (d\lambda_i(g) + \lambda_i(g)w)c$ and $g \to \lambda_i(g)c$ is continuous on $g_i U$ for each $c \in C^*(\mathfrak{G}, M)$. If we put $\phi_i(g)\lambda_i(g)c = 0$, $\{\phi_i\}$ a partition of unity refining the covering $\{g_i U\}$, for $g \notin g_i U$ then clearly $g \to \phi_i(g)\lambda_i(g)c$ is continuous on G_0, so if we put $\lambda(g)c = \sum_{i=1}^{n} \phi_i(g)\lambda_i(g)c$ then $g \to \lambda(g)c$ is continuous on U, and satisfies the requirements of the lemma.

8.2. LEMMA. *Let μ_0 be the normalized Haar measure on G_0. If M is a differentiable G-module, define $A : C^*(\mathfrak{G}, M) \to C^*(\mathfrak{G}, M)$ by $Ac = \int gc\, d\mu_0(g)$. Then there is a linear map λ of $C^*(\mathfrak{G}, M)$ into itself such that $Ac - c = d\lambda c + \lambda dc$ for all $c \in C^*(\mathfrak{G}, M)$.*

Proof. Define $\lambda c = \int (g)c\, d\mu_0(g)$ is chosen as in Lemma 8.1.

8.3. LEMMA. *Let M be a differentiable G-module and let $A : C^*(\mathfrak{G}, M) \to C^*(\mathfrak{G}, M)$ be the linear operator defined in Lemma 8.2. Then A has the following properties:*

(1) *It is a projection of $C^*(\mathfrak{G}, M)$ on $C_I^*(\mathfrak{G}, M)$.*

(2) *It commutes with d.*

(3) *If $z \in Z^*(\mathfrak{G}, M)$ then $Az - z \in B^*(\mathfrak{G}, M)$ i.e. Az is cohomologous to z.*

Proof. Property (1) follows directly from the invariance of Haar measure and statement (3) of 6.8 (applied to $C^*(\mathfrak{G}, M)$ instead of M). Statement (2) follows from the fact that d commutes with the operations of G on $C^*(\mathfrak{G}, M)$ and with the integral. Finally (3) is an immediate consequence of Lemma 8.2. q.e.d.

8.4. THE MAIN THEOREM. *If M is a derived $\mathfrak{G}$-module then the natural homomorphism $i^*: H_I^*(\mathfrak{G}, M) \to H^*(\mathfrak{G}, M)$ induced by the inclusion map of $C_I^*(\mathfrak{G}, M)$ in $C^*(\mathfrak{G}, M)$ is an isomorphism onto. In other words every cohomology class of $H^*(\mathfrak{G}, M)$ contains an invariant cocycle, and two invariant cocycles which differ by a coboundary differ by the coboundary of an invariant cochain.*

Proof. Immediate from 8.3.

8.5. COROLLARY. *If $\mathfrak{G}$ is semi-simple then $H^1(\mathfrak{G}, M) = H^2(\mathfrak{G}, M) = 0$ for all derived $\mathfrak{G}$-modules M.*

Proof. Immediate from 8.4 and the theorem of § 3.

9. The differentiability of tensor modules. Let $\mathfrak{M}$ be a differentiable G-space, i.e. $\mathfrak{M}$ is a differentiable ($= C^\infty$) manifold and there is given a differentiable map $(g, p) \to gp$ of $G \times \mathfrak{M}$ into $\mathfrak{M}$ (the *action* of G on $\mathfrak{M}$) such that $ep \equiv p$ and $(gg^1)p \equiv g(g^1p)$. For each $X \in \mathfrak{G}$ there is a differentiable vector field X^* on $\mathfrak{M}$ defined by X^*_p is the tangent to $t \to (\mathrm{Exp} - tX)p$ at $t = 0$. The map $X \to X^*$ is a homomorphism of $\mathfrak{G}$ into the Lie algebra of differentiable vector fields on $\mathfrak{M}$ which is called the *infinitesimal generator* of the action of G *on* $\mathfrak{M}$. Let $\mathfrak{T}$ be the space of all differentiable tensor fields on $\mathfrak{M}$ of any fixed (mixed) rank and symmetry type with the usual "C^∞-topology" (i.e. convergence means uniform convergence of each component and of each partial derivative of any order of a component on any compact subset of a coordinate neighborhood). It is well-known that $\mathfrak{T}$ is a complete locally convex space and in fact a Montel space. Moreover if $\mathfrak{M}$ is second countable, as we henceforth assume, then $\mathfrak{T}$ is metrizable. Each diffeomorphism ϕ of $\mathfrak{M}$ induces an automorphism of $\mathfrak{T}$ in a well-known way and we will write this automorphism as ϕ also. Moreover if $\{\phi_n\}$ is a sequence of diffeomorphism of $\mathfrak{M}$ converging to a diffeomorphism ϕ in the C^∞-topology then it is clear that $\phi_n T \to \phi T$ for any $T \in \mathfrak{T}$. By a theorem of Montgomery [4] if we write g^* for the operation $p \to gp$ of an element of G on $\mathfrak{M}$ then $g \to g^*$ is continuous from G into the group of diffeomorphisms of $\mathfrak{M}$ with the C^∞-topology. It follows from these last two facts that

$\mathcal{T}$ is a topological G-module if we define $gT = g^*T$. We shall call such a topological G-module a *module* of tensor fields (associated with the differentiable G-space $\mathfrak{M}$) and shall as usual write gT instead of g^*T. It follows easily from Theorem II of [5] that a module of tensor fields $\mathcal{T}$ is always differentiable and that for $X \in \mathfrak{g}$ and $T \in \mathcal{T}$ XT is just the usual Lie derivative of T with respect to the vector field X^*. We can now forget about the topology on $\mathcal{T}$ and even the action of G on $\mathcal{T}$. All that is important for the applications we shall make is summed up in

THEOREM. *Let $\mathfrak{M}$ be a differentiable G-space and $X \to X^*$ the infinitesimal generator of the action of G on $\mathfrak{M}$. Let $\mathcal{T}$ be the space of all differentiable tensor fields on $\mathfrak{M}$ of a fixed rank and symmetry type, and for $X \in \mathfrak{g}$ and $T \in \mathcal{T}$ let XT be the Lie derivative of T with respect to X^*. Then this makes $\mathcal{T}$ into a derived $\mathfrak{g}$-module so that* (8.4 and 8.5) $H^*(\mathfrak{g}, \mathcal{T}) \cong H_I^*(\mathfrak{g}, \mathcal{T})$ *and if $\mathfrak{g}$ is semi-simple* $H^1(\mathfrak{g}, \mathcal{T}) = H^2(\mathfrak{g}, \mathcal{T}) = 0$.

10. $H^*(G, R) \cong H^*(\mathfrak{g})$ as a special case. Consider G as a differentiable G-space under the map $(g, p) \to pg^{-1}$. Then for each $X \in \mathcal{T}$ the associated vector field X^* on G is just X itself. Let $\mathcal{T}$ be the tensor module of all differentiable real valued functions on G. If ω is a p-form on G then ω defines an element c of $C^p(\mathfrak{g}, \mathcal{T})$ by $c(X_1, \cdots, X_p)(x) = \omega_x((X_1)_x, \cdots, (X_p)_x)$. Conversely given $c \in C^p(\mathfrak{g}, \mathcal{T})$ define a p-form ω on G as follows: given $x \in G$ and tangent vectors $Y_1, \cdots, Y_p$ at x let $\omega_x(Y_1, \cdots, Y_p) = c(X_1, \cdots, X_p)(x)$ where X_i is the element of $\mathfrak{g}$ satisfying $(X_i)_x = Y_i$. It is readily verified that ω is differentiable and that these two maps are mutually inverse linear isomorphisms between $C^*(\mathfrak{g}, \mathcal{T})$ and the space $\Omega_0(G)$ of differentiable forms on G. Moreover it is a well-known fact (a proof can be found in [15]) that under this correspondence the differential on $C^*(\mathfrak{g}, \mathcal{T})$ corresponds to the exterior derivative on $\Omega^*(G)$. Thus by deRham's Theorem $H^*(G, R) \cong H^*(\mathfrak{g}, \mathcal{T})$ and so by the theorem of § 9 $H^*(G, R) \cong H_I^*(\mathfrak{g}, \mathcal{T})$. For $c \in C^p(\mathfrak{g}, \mathcal{T})$ we have

$$(gc)(X_1, \cdots, X_p)(x) = c(ad(g^{-1})X_1, \cdots, ad(g^{-1})X_p)(xg)$$

and if $X \in \mathfrak{g}$ then by left invariance $(ad(g^{-1})X)_{xg} = dRg(X_x)$ (where Rg is right translation by g). It follows that $c \in C_I^*(\mathfrak{g}, \mathcal{T})$ if and only if the corresponding form ω is right invariant. This gives the well-known identification of $H^*(G, R)$ with the cohomology of right invariant forms (form of Maurer-Cartan). On the other hand we see that each $c \in C^p(\mathfrak{g})$ corresponds to a unique $c' \in C_I^p(\mathfrak{g}, \mathcal{T})$ such that $c(X_1, \cdots, X_p) = c'(X_1, \cdots, X_p)(e)$; namely $c'(X_1, \cdots, X_p)(g) = c(ad(g)X_1, \cdots, ad(g)X_p)$. This sets up a linear isomorphism between $C^*(\mathfrak{g})$ and $C_I{}^*(\mathfrak{g}, \mathfrak{I})$ and referring to equations (5) and (6) of § 1 we see that d_T corresponds to $-d_I$ under this isomorphism. It follows that $H_I{}^*(\mathfrak{g}, \mathfrak{I}) \cong H^*(\mathfrak{g})$ and this gives the well-known result $H^*(G, R) \cong H^*(\mathfrak{g})$. In [2], where the cohomology theory of Lie algebras was first made explicit, there is a detailed account of theorems of this general nature.

11. Infinitesimal deformation of differentiable G-spaces. Let $\mathfrak{M}$ be a differentiable G-space, $\Phi\colon G \times \mathfrak{M} \to \mathfrak{M}$ the action of G on $\mathfrak{M}$ and $X \to X^*$ the infinitesimal geenrator of Φ. Suppose that for each $t \in [0,1] = I$ there is given an action Φ_t of G on $\mathfrak{M}$ such that $\Phi_0 = \Phi$ and such that $(g, p, t) \to \Phi_t(g, p)$ is a differentiable map of $G \times \mathfrak{M} \times I$ into $\mathfrak{M}$. Such a family Φ_t will be called a *deformation* of Φ and we write $X \to X_t{}^*$ for the infinitesimal generator of Φ_t. It is easily seen that $(X, p, t) \to (X_t{}^*)_p$ is a differentiable map of $\mathfrak{g} \times \mathfrak{M} \times I$ into the tangent bundle of $\mathfrak{M}$ and it follows that for each $X \in \mathfrak{g}$ there is a differentiable vector field DX on $\mathfrak{M}$ such that $(DX)_p = \left.\dfrac{d}{dt}\right|_{t=0} (X_t{}^*)_p$. Clearly D is a linear map of $\mathfrak{g}$ into the Lie algebra $\mathfrak{V}$ of differentiable vector fields on $\mathfrak{M}$ and since $[X, Y]_t{}^* = [X_t{}^*, Y_t{}^*]$ it follows that $D([X, Y]) = [DX, Y^*] + [X^*, DY]$. We call D the infinitesimal deformation of Φ associated with Φ_t and in general a linear map $D'\colon \mathfrak{g} \to \mathfrak{V}$ satisfying the above identity is called an infinitesimal deformation of Φ. Now if Φ_t is a deformation of $\mathfrak{M}$ (i. e. $(p, t) \to \Phi_t(p)$ is a differentiable map of $\mathfrak{M} \times I \to \mathfrak{M}$ and for each $t \in I$ ϕ_t is a diffeomorphism of $\mathfrak{M}$) the vector field Z defined by $Z_p =$ tangent to $t \to \Phi_t(p)$ at $t = 0$ is called the infinitesimal deformation of $\mathfrak{M}$ associated with ϕ_t. From ϕ_t we can construct a deformation Φ_t of Φ by $\Phi_t(g, p) = \phi_t(\Phi(g, \phi_t{}^{-1}(p)))$. A deformation of Φ that can be defined in this way is called *trivial*. It is easily seen that the associated infinitesimal deformation D of Φ is given by $DX = [Z, X^*] = ad(Z)X^*$ where Z as above is the infinitesimal deformation of $\mathfrak{M}$ associated with ϕ_t. In general if $Z' \in \mathfrak{V} D'\colon X \to ad(Z')X^*$ is an infinitesimal deformation of Φ and we call such infinitesimal deformations of Φ *trivial* (at least if $\mathfrak{M}$ is compact Z' is the infinitesimal deformation of $\mathfrak{M}$ associated with some deformation ϕ_t of $\mathfrak{M}$ so in this case D' is the infinitesimal deformation of Φ associated with a trivial deformation of Φ). Now consider $\mathfrak{V}$ as a tensor module associated to the G-space $\mathfrak{M}$ and recall that the Lie derivative of $Y \in \mathfrak{V}$ with respect to $Z \in \mathfrak{V}$ is just $[Z, Y]$ (see, for example [5] Lemma c). It follows that $\mathfrak{V}$ is a derived $\mathfrak{g}$ module under the operations $XY = [X^*, Y]$. Now an element of $C^1(\mathfrak{g}, \mathfrak{V})$ is just a linear map $c\colon \mathfrak{g} \to \mathfrak{V}$ and $c \in Z'(\mathfrak{g}, \mathfrak{V})$

if and only if $0 \equiv dc(X,Y) = Xc(Y) - Yc(X) - c([X,Y])$ i.e. if and only if $c([X,Y]) = [X^*, c(Y)] + [c(X), Y^*]$. Thus $Z'(\mathfrak{G},\mathfrak{V})$ is just the space of infinitesimal deformations of Φ. On the other hand $c \in D'(\mathfrak{G},\mathfrak{V})$ if and only if for some $Z \in \mathfrak{V} c(X) \equiv dZ(X) = X(Z) - [-Z, X^*]$ i.e. if and only if c is a trivial infinitesimal deformation of Φ. Thus $H^1(\mathfrak{G},\mathfrak{V}) = 0$ means every infinitesimal deformation of Φ is trivial. Since $\mathfrak{V}$ is a tensor module it follows from the Theorem of § 9 that

11.1. THEOREM. *If G is a compact semi-simple Lie group then every infinitesimal deformation of the action of G on a differentiable G-space is trivial.*

In [7] the authors prove a global form of this theorem; namely that if G is any compact Lie group (not necessarily semi-simple) then every deformation of the action of G on a compact differentiable G-space is trivial. It does not seem that either of these theorems implies the other in any obvious way.

Now let $\mathfrak{L}$ be a finite dimensional subalgebra of the Lie algebra $\mathfrak{V}$ of all differentiable vector fields on a compact differentiable manifold $\mathfrak{M}$. If $\mathfrak{V}$ is a compact semi-simple Lie algebra (i.e. the Killing form is negative definite) then the simply connected Lie group G with Lie algebra $\mathfrak{G}$ isomorphic to $\mathfrak{L}$ is compact and semi-simple. By Corollary 2 of Theorem XVIII of [6] an isomorphism of $\mathfrak{G}$ onto $\mathfrak{L}$ is the infinitesimal generator of an action of G on $\mathfrak{M}$. Applying 11.1

11.2. THEOREM. *If $\mathfrak{L}$ is a compact semi-simple sub-algebra of the Lie algebra $\mathfrak{V}$ of differentiable vector fields on a compact differentiable manifold, then every derivation of $\mathfrak{L}$ into $\mathfrak{V}$ is the restriction to $\mathfrak{L}$ of an inner derivation of $\mathfrak{V}$.*

12. Lifting of group actions. In this section we assume that our compact Lie group G is connected and denote by $\tilde{G}$ its simply connected covering group. We shall identify the Lie algebras of G and $\tilde{G}$ under the isomorphism given by the differential of the covering homomorphism. We note that a differentiable G-space $\mathfrak{M}$ is in a natural way a differentiable $\tilde{G}$-space and that the homomorphisms of $\mathfrak{G}$ into the Lie algebra $\mathfrak{V}$ of differentiable vector fields on $\mathfrak{M}$ which are the infinitesimal generators of the actions of G and $\tilde{G}$ on $\mathfrak{M}$ are the same.

In general a homomorphism $X \rightarrow X^*$ of $\mathfrak{G}$ into $\mathfrak{V}$ is not the infinitesimal generator of an action of G or even $\tilde{G}$ on $\mathfrak{M}$ if $\mathfrak{M}$ is not compact. However it is shown in [6, Theorem III, p. 95] that if each of the vector fields X^* generates a global one-parameter group of diffeomorphism of $\mathfrak{M}$ then $X \rightarrow X^*$

is the infinitesimal generator of a unique action of $\tilde{G}$ on $\mathfrak{M}$. Now if X^* does not generate a global one parameter group of diffeomorphism of $\mathfrak{M}$ then (for example, see [6, p. 84 and p. 73]) there is an integral curve σ of X^* defined on an intevral $[0,a)$ or $(a,0]$ such that $\lim_{t\to a}\sigma(t)=\infty$ (i.e. for each compact subset K of $\mathfrak{M}$ $\sigma(t)\notin K$ for t sufficiently close to a). Suppose now Y is a vector field on a differentiable manifold $\mathfrak{N}$, X a vector field on $\mathfrak{M}$ and $f\colon \mathfrak{N}\to\mathfrak{M}$ is a differentiable map such that $df(Y_p)\equiv X_{f(p)}$ (under these circumstances we say, following Chevalley [1, p. 84] that Y and X are f-related). Then if σ is an integral curve of Y $f\circ\sigma$ is an integral curve of X and it follows from the above remark that if X generates a global one parameter group of diffeomorphisms of $\mathfrak{M}$ and if f is proper then Y generates a global one parameter group of diffeomorphisms of $\mathfrak{N}$.

Now let $X\to X^*$ be the infinitesimal generator of the action of G on a differentiable G-space $\mathfrak{M}$ and let π be the projection of a differentiable fiber bundle B over $\mathfrak{M}$, having compact fiber. Then π is proper and it follows that there is a one-to-one correspondence between actions of $\tilde{G}$ on B for which π is equivariant and homomorphisms $\tau\colon X\to X^\tau$ of $\mathfrak{G}$ into the Lie algebra of differentiable vector fields on $\mathfrak{M}$ such that X^τ and X^* are π-related for all $X\in\mathfrak{G}$. We now specialize further and assume that B is a principle-bundle with structural group a compact connected Lie group H and we write $(h,b)\to hb$ for the action of H on B (this conflicts with the more customary usage in which the structural group acts on the right, but it is only necessary to define hb to be bh^{-1}).

For a diffeomorphism of B to be a bundle map, i.e. equivariant with respect to the action of H, means just that it commutes with each operation of H; hence if $Z\to Z^*$ is the homomorphism of the Lie algebra $\mathfrak{H}$ of H into the differentiable vector fields on B which generates the action of H, then a one parameter group of diffeomorphism of B consists of bundle maps if and only if its infinitesimal generator Y satisfies $[Y,Z^*]=0$ for all $Z\in\mathfrak{H}$. Thus

12.1. THEOREM. *Let $X\to X^*$ be the infinitesimal generator of the action of G on a differentiable G-space $\mathfrak{M}$. Let H be a compact connected Lie group with Lie algsbra $\mathfrak{H}$, B a differentiable principle H-bundle over $\mathfrak{M}$ with projection π and $Z\to Z^*$ the infinitesimal generator of the action of H on B. Then there is a one-to-one correspondence between actions of $\tilde{G}$ on B equivariant with respect to π such that each operation of $\tilde{G}$ on B is a bundle equivalence, and homomorphisms $\tau\colon X\to X^\tau$ of $\mathfrak{G}$ into the Lie algebra of differentiable vector fields on B such that*

(1) *X^τ and X^* are π-related for all $X\in\mathfrak{G}$*

(2) *$[X^\tau,Z^*]=0$ for all $X\in\mathfrak{G}$, $Z\in\mathfrak{H}$.*

A homomorphism $\tau\colon X \to X^{\tau}$ satisfying (1) and (2) will be called a lifting of $\mathfrak{G}$ to B. A linear map $\tau\colon X \to X^{\tau}$ of $\mathfrak{G}$ into the Lie algebra of differentiable vector fields on B which satisfies these conditions will be called a *pseudo-lifting* of $\mathfrak{G}$ to B. To construct a pseudo-lifting of $\mathfrak{G}$ to B it is only necessary to choose an H-invariant Riemannian-metric for B and let $X_b{}^{\tau}$ be the unique vector at b orthogonal to the fibre which projects onto $X^*{}_{\pi(b)}$. It is easily checked that X^{τ} is differentiable and by construction it is π-related to X^*. That X^{τ} is H-invariant and hence commutes with Z^* for all $Z \in \mathfrak{H}$ follows from the invariance of the metric. Liftings of $\mathfrak{G}$ to B on the other hand need not always exist and one of the principle results of this section is that they in fact do exist (and are essentially unique) if H is a torus and G is semi-simple. In general we have the relation $Z^*{}_{hb} = dh(ad(h^{-1})Z)^*{}_b$ for $Z \in \mathfrak{H}$, $h \in H$. We now make a final simplifying assumption, namely that H is a torus so that it follows from the above relation that Z^* is an H-invariant vector field on B for all $Z \in \mathfrak{H}$. A vector field Y on B is called *vertical* if $\delta\pi(Y) = 0$ (i.e. Y is π-related to zero). Clearly for each $p \in \mathfrak{M}$ $Z \to Z^*|\pi^{-1}(p)$ is an isomorphism of $\mathfrak{H}$ with the space of vertical H-invariant vector fields on $\pi^{-1}(p)$. It follows that every vector field Y on B which is vertical and H-invariant is of the form $b \to (f(\pi(b)))^*{}_b$ for a uniquely determined function $f\colon \mathfrak{M} \to \mathfrak{H}$, moreover Y is differentiable if and only if f is differentiable (the latter meaning of course that $l \circ f$ is differentiable for every linear functional l on $\mathfrak{H}$). It follows that we may identify the space M of differentiable maps of $\mathfrak{M}$ into $\mathfrak{H}$ with the space of all vertical vector fields on B which are H-invariant (or, equivalently, which commute with Z^* for all $Z \in \mathfrak{H}$). We note that since $\mathfrak{H}$ is abelian any two elements of M, considered as vertical vector fields, commute. If Y is a vector field on $\mathfrak{M}$ and $m \in M$ then Ym is a well defined element of M; namely its value $(Ym)(p)$ at $p \in \mathfrak{M}$ is the unique element of $\mathfrak{H}$ such that $l((Ym)(p)) = Yp(l \circ m)$ for each linear functional l on $\mathfrak{H}$. Moreover by considering local product representations of B it is easily seen that if Y' is a vector field on B π-related to Y then $Ym = [Y', m]$. Clearly M becomes a $\mathfrak{G}$-module if we define $Xm = X^*{}_m$ for $X \in \mathfrak{G}$, $m \in M$. Moreover from the previous remark $Xm = [X^{\tau}, m]$ if $\tau\colon X \to X^{\tau}$ is any pseudo-lifting of $\mathfrak{G}$ to B. If $\mathfrak{F}$ is the tensor module of differentiable real valued functions on $\mathfrak{M}$ and $X_1, \cdots, X_n$ is a basis for $\mathfrak{H}$ then $(f_1, \cdots, f_n) \to f_1X_1 + \cdots + f_nX_n$ (where the latter means the elment of M whose value at p is $\sum f_i(p)X_i$) is an isomorphism (as $\mathfrak{G}$-modules) of the n-fold direct sum of $\mathfrak{F}$ with itself and M. It follows from the theorem of § 9 that $H^*(\mathfrak{G}, M) \cong H_I(\mathfrak{G}, M)$ and that if G is semi-simple then $H^1(\mathfrak{G}, M) = H^2(\mathfrak{G}, M) = 0$. We collect these results as

12.2. THEOREM. *With the assumptions of* 12.1 *and the additional assumption that* H *is a torus let* M *be the linear space of differentiable maps of* $\mathfrak{M}$ *into* $\mathfrak{H}$. *If we identify* $m \in M$ *with the vector field on* B *whose value at* b *is* $(m(\pi(b))^*)_b$ *then this gives a linear isomorphism of* M *with the linear space of differentialble vertical vector fields on* B *which commute with* Z^* *for all* $Z \in \mathfrak{H}$. *Considered as vertical vector fields on* B *any two elements of* M *commute. Moreover* M *is a* $\mathfrak{G}$*-module satisfying* $H^*(\mathfrak{G},M) = H^*_I(\mathfrak{G},M)$ *(and hence* $H^1(\mathfrak{G},M) = H^2(\mathfrak{G},M) = 0$ *if* G *is semi-simple) the module structure being characterized by the relation* $Xm = [X^\tau, m]$ if $\tau\colon X \to X^\tau$ *is any pseudo-lifting of* $\mathfrak{G}$ *to* B.

Continuing now with the same assumptions, with each pseudo-lifting $\tau\colon X \to X^\tau$ of $\mathfrak{G}$ to B we associate a map c_τ of $\mathfrak{G} \times \mathfrak{G}$ into vector fields on B by $c_\tau(X,Y) = [X^\tau, Y^\tau] - [X,Y]^\tau$. Clearly c_τ is a measure of how much τ fails to be a lifting, i.e. $c_\tau \equiv 0$ if and only if τ is a lifting. Now $[X,Y]^\tau$ is π-related to $[X,Y]^*$ and by [1, p. 85] $[X^\tau, Y^\tau]$ is π-related to $[X^*; Y^*] = [X,Y]^*$. It follows that $c_\tau(X,Y)$ is π-related to 0, i.e. is vertical. Since $[X,Y]^\tau$ and $[X^\tau, Y^\tau]$ commute with Z^* for all $Z \in \mathfrak{H}$ ($[X,Y]^\tau$ by definition of a pseudo-lifting, $[X^\tau, Y^\tau]$ by the same plus the Jacobi identity) so does $c_\tau(X,Y)$, hence we can identify $c_\tau(X,Y)$ with an element of M. Moreover c_τ is clearly bilinear and skew-symmetric and hence an element of $C^2(\mathfrak{G},M)$ If X_1, X_2, X_3 belong to $\mathfrak{G}$ then

$$
\begin{aligned}
[X_1{}^\tau, [X_2{}^\tau, X_3{}^\tau]] &= [X_1{}^\tau, [X_2, X_3]^\tau + c_\tau(X_2, X_3)] \\
&= [X_1, [X_2, X_3]]^\tau + c_\tau(X_1, [X_2, X_3]) + X_1 c_\tau(X_2, X_3)
\end{aligned}
$$

Now $[X_1{}^\tau, [X_2{}^\tau, X_3{}^\tau]]$ satisfies the Jacobi identity, i.e. its sum with its two cyclic permutations is zero. Since τ is linear so does $[X_1, [X_2, X_3]]^\tau$. Writing out the cyclic permutations of the above equation and summing we get an equation which gives $dc_\tau(X_1, X_2, X_3) = 0$, hence $c_\tau \in Z^2(\mathfrak{G},M)$. We call c_τ the *error cocycle* of the pseudo-lifting τ.

Now let $\gamma \in C^1(\mathfrak{G},M)$, i.e. γ is a linear map of $\mathfrak{G}$ into M. Then it is clear that $\sigma\colon X \to X^\sigma = X^\tau + \gamma(X)$ is another pseudo-lifting of $\mathfrak{G}$ to B and that conversely every pseudo lifting of $\mathfrak{G}$ to B is of this form for a unique $\gamma \in C^1(\mathfrak{G},M)$. We call γ the difference cochain of σ and τ. Recalling from 12.2 that $[\gamma(X), \gamma(Y)] = 0$ for $X, Y \in \mathfrak{G}$

$$
\begin{aligned}
c_\sigma(X,Y) &= [X^\tau + \gamma(X), Y^\tau + \gamma(Y)] - [X,Y]^\tau - \gamma([X,Y]) \\
&= [X^\tau, Y^\tau] - [X,Y]^\tau - \gamma([X,Y] + X\gamma(Y) - Y\gamma(X) \\
&= c_\tau(X,Y) + d\gamma(X,Y)
\end{aligned}
$$

or in words, the difference of the error cocycles c_σ and c_τ is just the coboundary of the difference cochain $\gamma = \sigma - \tau$. Thus the set of error cocycles associated with pseudo-liftings of $\mathfrak{G}$ to B is an entire cohomology class $\omega \in H^2(\mathfrak{G}, M)$ which we call the *obstruction to a lifting of* $\mathfrak{G}$ *to* B. By what we have seen above a lifting of $\mathfrak{G}$ to B exists if and only if ω contains the zero element, thus we have the only apparently tautological statement

12.3. THEOREM. *If B is a principle torus bundle over a differentiable G-space $\mathfrak{M}$, then a lifting of $\mathfrak{G}$ to B exists if and only if the obstruction to a lifting of $\mathfrak{G}$ to B vanishes.*

Since $\omega \in H^2(\mathfrak{G}, M)$ which by 12.2 is zero if G is semi-simple.

12.4. COROLLARY. *If G is a compact semi-simple Lie group and B is a principle torus bundle over a differentiable G-space $\mathfrak{M}$ then there is a lifting of $\mathfrak{G}$ to B.*

We now consider the uniqueness problem for liftings of $\mathfrak{G}$ to B. Returning to our general situation let σ and τ be two liftings of $\mathfrak{G}$ to B. Their difference cochain γ is clearly a one-cocycle. Conversely $\gamma \in Z^1(\mathfrak{G}, M)$ and τ is a lifting of $\mathfrak{G}$ to B then so is $\sigma = \tau + \gamma$. Assume now that the obstruction cocycle ω is zero so that a lifting τ of $\mathfrak{G}$ to B exists and assume also that $H^1(\mathfrak{G}, M) = 0$ so that by the above remark every lifting σ of $\mathfrak{G}$ to B is of the form $\tau + dm$ for some $m \in M = C^0(\mathfrak{G}, M)$. More explicitly $X^\sigma = X^\tau + Xm = X^\tau + [X^\tau, m]$.

The most general bundle equivalence of B is of the form $b \to f(\pi(b))b$ when f is a differentiable map of $\mathfrak{M}$ into H. Since $\mathrm{Exp}\colon \mathfrak{H} \to H$ is the universal covering map of H it follows that every such f can be written in the form $\mathrm{Exp} \circ m$ for some $m \in M$. Moreover by taking a local product representation of B it is easily seen that if h is the bundle equivalence given by $b \to (\mathrm{Exp}(m(\pi(b)))b$ then $dh(X^\tau{}_{h^{-1}(b)}) = (X^\tau + Xm)_b$ i.e. $X^\sigma = dh \circ X^\tau \circ h^{-1}$. It follows that if $(g, b) \to gb$ is the action of $\tilde{G}$ on B generated by X^τ then the action generated by X^σ is $(gb) \to hgh^{-1}(\mathrm{b})$. Since $H^1(\mathfrak{G}, M) = 0$ if G is semi-simple combining these remarks with 12.1 and 12.4 we have

12.5. THEOREM. *If G is a semi-simple compact Lie group, $\mathfrak{M}$ a differentiable G-space, and B a torus bundle over $\mathfrak{M}$, then there is a differentiable action $(g, b) \to gb$ of $\tilde{G}$ on B which is equivariant with respect to the projection of B on $\mathfrak{M}$ and is such that each operation of $\tilde{G}$ on B is a bundle map. Moreover this action is essentially unique in the sense that every other such* *action of $\tilde{G}$ on B is of the form $(g,b) \rightarrow hgh^{-1}b$ where h is a differentiable bundle equivalence of B.*

The latter theorem can be significantly generalized as follows

12. 6. THEOREM. *Let G be a simply connected compact Lie group, H a solvable, connected Lie group, $\mathfrak{M}$ a differentiable G-space and B a differentiable principle H-bundle over $\mathfrak{M}$. Then there is a differentiable action of G on B such that the projection of B on $\mathfrak{M}$ is equivariant and each operation of G on B is a bundle map. Moreover this action is essentially unique in the sense that any other action of G on B with these properties is related by conjugation with a bundle equivalence as in* 12. 5.

Proof. By induction on $\dim H$. If $\dim H = 1$ then either H is a circle group and the theorem is a consequence of 12. 5 or else H is isomorphic to the additive group of real numbers. In the latter case H is solid so that [8, p. 55] B is a product bundle so that existence of the required type of action of G on B is obvious. Uniqueness can be proved just as in 12. 5. Now suppose $\dim H > 1$ and that the theorem holds for all H of smaller dimension. Then H has a closed normal subgroup N such that both N and H/N are conected solvable Lie groups of dimension smaller than that of H. Now B is a principle N-bundle over the orbit space B/N and B/N is a principle H/N bundle over $\mathfrak{M}$ and the composition of the projections $B \rightarrow B/N \rightarrow \mathfrak{M}$ is just the bundle projection $B \rightarrow \mathfrak{M}$. By the induction hypothesis we can lift the action of G—first to B/N and then to B. Moreover any action of the apropriate sort on B induces one on B/N. Since the liftings from $\mathfrak{M}$ to B/N and from B/N to B are essentially unique by the induction hypothesis, the same follows easily for the lifting from $\mathfrak{M}$ to B.

BRANDEIS UNIVERSITY
AND
THE INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[1] C. Chevalley, *Theory of Lie Groups*, Princeton University Press, Princeton, 1946.

[2] C. Chevalley and S. Eilenberg, "Cohomology theory of Lie groups and Lie algebras," *Transactions of the American Mathematical Society*, vol. 63 (1948), pp. 85-124.

[3] G. Hochschild and J-P. Serre, "Cohomology of Lie algebras," *Annals of Mathematics*, vol. 57 (1953), p. 591.

[4] D. Montgomery, "Topological groups of differentiable transformations," *Annals of Mathematics*, vol. 46 (1945), pp. 382-387.

[5] R. Palais, "A definition of the exterior derivative in terms of Lie derivatives," *Proceedings of the American Mathematical Society*, vol. 5 (1954), pp. 902-908.

[6] ———, "A global formulation of the Lie theory of transformation groups," *Memoirs of the American Mathematical Society*, No. 22 (1957).

[7] R. Palais and T. Stewart, "Deformations of compact, differentiable transformation groups," *American Journay of Mathematics*. To appear.

[8] N. Steenrod, *The Topology of Fiber Bundles*, Princeton University Press, Princeton, 1951.

[9] T. Stewart, "Lifting the action of a group in a fiber bundle," *Bulletin of the American Mathematical Society*, vol. 66 (1960), pp. 129-132.

[10] J. H. C. Whitehead, "Certain equations in the algebra of semi-simple infinitesimal groups," *Quarterly Journal of Mathematics* (1937), p. 220.

[11] ———, "On the decomposition of an infinitesimal group," *Proceedings of the Cambridge Philosophical Society*, vol. 32 (1936), p. 229.

AN INVARIANT CRITERION OF HYPOELLIPTICITY.*

By FRANÇOIS TREVES.†

Introduction. A differential operator $\boldsymbol{P}$ on a C^∞ manifold Ω is said to be *hypoelliptic* in Ω if, whatever be the distribution u on Ω, u has to be a C^∞ function in any open set in which $\boldsymbol{P}u$ is a C^∞ function.

Several sufficient conditions of hypoellipticity have been given, from classical ones: the elliptic operators are hypoelliptic and so are the parabolic ones, to more recent (and weaker!) like the formal hypoellipticity, introduced by Lars Hörmander and Bernard Malgrange. Beside ellipticity, none of those sufficient conditions is invariant: they are properties of the expression of the operator in a system of coordinates which do not subsist when one changes coordinates.

Since the definition of hypoellipticity is itself obviously invariant, it was natural to look for invariant conditions. In the present paper, we define a class of differential operators, which we call *regular,* by invariant a priori estimates, and we prove that a regular operator is hypoelliptic.

This result can be considered only as a first step on a difficult road. For what one should wish, is to have properties of the expression of the differential operator in *any* system of local coordinates which insure hypoellipticity; and that we do not provide. However, in the last section, we prove rapidly that any formally hypoelliptic operator is regular.

The main step in our proof consists in deriving estimates about the commutator $[\boldsymbol{P}, \rho_\epsilon{}^*]$ of the differential operator $\boldsymbol{P}$ with Friedrichs mollifiers from "similar" estimates about the commutator $[\boldsymbol{P}, \boldsymbol{Q}]$ of $\boldsymbol{P}$ with arbitrary differential operators $\boldsymbol{Q}$ (§ 6). This could be of interest in questions which do not bear any relation to hypoellipticity.

Let us also mention that the reading of the article does not require any knowledge about distributions but the most superficial.

1. Differential operators and their derivatives. Let Ω be a C^∞ manifold of dimension $n \geqq 1$. As usual $C^\infty(\Omega)$ will denote the vector space of C^∞ complex valued functions on Ω. A differential operator $\boldsymbol{P}$ on Ω is a linear map of $C^\infty(\Omega)$ into itself which satisfies the following conditions:

---

* Received April 27, 1961.

† The author is a Fellow of the Sloan Foundation.

$(DO_I)_I$ For every compact subset K of Ω there is an integer $M_K \geqq 0$ such that if all the derivatives of $\phi \in C^\infty(\Omega)$ of order $\leqq M_K$ converge to zero uniformly on K, $\boldsymbol{P}\phi \to 0$ uniformly on K.

(DO_{II}) The support of $\boldsymbol{P}\phi$ is contained in the support of ϕ.[1]

We denote by ω the variable point in Ω. If T is a letter, ϕ any element of $C^\infty(\Omega)$, it follows from (DO_I) that, on every compact subset of Ω,

$$e^{-T\phi(\omega)}\boldsymbol{P}(e^{T\phi(\omega)})$$

is a polynomial in T of degree $m(\phi,\omega)$ depending on ϕ and on the point ω; $m(\omega) = \sup m(\phi,\omega)$ is *the order of* $\boldsymbol{P}$ *at* ω. For any subset A of Ω, $\sup_{\omega\in A} m(\omega)$ is *the order of* $\boldsymbol{P}$ *in* A; observe that it could be infinite (it is certainly finite when A is compact). In this article we shall *not* make the assumption that $m(\omega)$ is independent of ω.

Let Ω' be an open subset of Ω covered by local coordinats $(x^1,\cdots,x^n)$. In Ω' we may look at the partial differentiations $\frac{\partial}{\partial x^1},\cdots,\frac{\partial}{\partial x^n}$ and their products which we shall write

$$D_\alpha = \left(\frac{1}{2i\pi}\frac{\partial}{\partial x^{\alpha_1}}\right)\cdots\left(\frac{1}{2i\pi}\frac{\partial}{\partial x^{\alpha_r}}\right);$$

the α_j are integers and $1 \leqq \alpha_j \leqq n$; we set $\alpha = (\alpha_1,\cdots,\alpha_r)$ and r, which is called the *length* of α, will be denoted by $|\alpha|$. If $\phi \in C^\infty(\Omega')$, then for $x \in \Omega'$

$$\boldsymbol{P}\phi(x) = \sum A_\alpha(x)D_\alpha\phi(x);$$

here x can be regarded as the vector $(x^1,\cdots,x^n)$; the coefficients $A_\alpha(x)$ are C^∞ functions of x; for every x the summation is performed over a finite set of multi-indices α, actually over those α satisfying $|\alpha| \leqq m(x)$. The "differential operator" $\sum A_\alpha(x)D_\alpha$ is the *expression* of $\boldsymbol{P}$ in the coordinates $(x^1,\cdots,x^n)$; we shall usually denote it by $P(x,D)$.

To the expression $P(x,D)$ we may associate the polynomial (with coefficients in $C^\infty(\Omega')$)

$$P(x,\xi) = \sum A_\alpha(x)\xi_\alpha, \qquad \xi_\alpha = \xi_{\alpha_1}\cdots\xi_{\alpha_r};$$

and $\deg P(x,\xi) = m(x)$. If $\beta = (\beta_1,\cdots,\beta_s)$, $1 \leqq \beta_j \leqq n$, we set:

$$P^{(\beta)}(x,\xi) = \left(\frac{1}{2i\pi}\frac{\partial}{\partial\xi_{\beta_1}}\right)\cdots\left(\frac{1}{2i\pi}\frac{\partial}{\partial\xi_{\beta_s}}\right)P(x,\xi);$$

$$P_{(\beta)}(x,\xi) = \left(\frac{\partial}{\partial x^{\beta_1}}\right)\cdots\left(\frac{\partial}{\partial x^{\beta_s}}\right)P(x,\xi).$$

---

[1] Mr. J. Peetre has proved that (DO_{II}) implies (DO_I). See J. Peetre, "Une caractérisation abstraite des opérateurs différentiels," *Math. Scand.*, vol. 7 (1959), p. 211.

If $\boldsymbol{Q}$ is another differential operator in Ω', these notations allow us to express the commutator $[\boldsymbol{P}, \boldsymbol{Q}]$ in the coordinates $x^1, \cdots, x^n$:

$$(1.0) \qquad [\boldsymbol{P}, \boldsymbol{Q}] = \sum_{|\beta|+|\gamma|>0} \frac{(-1)^{|\gamma|}}{|\beta|!\,|\gamma|!} Q_{(\beta)}{}^{(\gamma)}(x, D)\, P_{(\gamma)}{}^{(\beta)}(x, D).$$

The proof of (1.0) is of course elementary. Let us derive from it two important particular cases. First we take $\boldsymbol{Q}$ of order zero; $\boldsymbol{Q}$ is then simply the multiplication by a C^∞ function ψ (on Ω'). Then (see Hörmander [1]):

$$(1.1) \qquad [\boldsymbol{P}, \boldsymbol{Q}] = \sum_{|\beta|>0} \frac{1}{|\beta|!} \frac{\partial \psi}{\partial x^\beta} P^{(\beta)}(x, D).$$

We use here, for simplicity, the notation

$$\frac{\partial}{\partial x^\beta} = \frac{\partial}{\partial x^{\beta_1}} \cdots \frac{\partial}{\partial x^{\beta_s}};$$

we have $\dfrac{\partial}{\partial x^\beta} = (2i\pi)^{|\beta|} D_\beta$.

Second, let us assume that the expression of $\boldsymbol{Q}$ in the coordinates x^j is a polynomial $Q(D)$ in $\dfrac{\partial}{\partial x^1}, \cdots, \dfrac{\partial}{\partial x^n}$ with *constant* coefficients. Then:

$$(1.2) \qquad [\boldsymbol{P}, \boldsymbol{Q}] = \sum_{|\beta|>0} \frac{(-1)^{|\beta|}}{|\beta|!} Q^{(\beta)}(D) P_{(\beta)}(x, D).$$

We want to derive from (1.1) and (1.2) two other formulas which will be useful later.

For that, we need to put an order relation (actually, a pre-order relation) on the multi-indices β. Let $\alpha = (\alpha_1, \cdots, \alpha_r)$, $\beta = (\beta_1, \cdots, \beta_s)$, $1 \leqq \alpha_j \leqq n$, $1 \leqq \beta_k \leqq n$ be two such multi-indices. We say that $\beta \leqq \alpha$ if, for every $p = 1, \cdots, n$, the number of β_k equal to p is $\leqq$ number of α_j equal to p. If $\alpha \leqq \beta$ and $\beta \leqq \alpha$, we write $\alpha \sim \beta$: α and β are then identical modulo a permutation. If $\beta \leqq \alpha$ without $\alpha \leqq \beta$, we write $\beta < \alpha$. With those notations:

$$\boldsymbol{P}(x^\alpha \phi) = \sum_{\beta \leqq \alpha} \frac{1}{|\beta|!} \frac{\partial}{\partial x^\beta}(x^\alpha) P^{(\beta)}(x, D)\phi, \ \phi \in C^\infty(\Omega'), \ x^\alpha = x^{\alpha_1} \cdots x^{\alpha_r}.$$

Also:

$$\sum_{\beta \sim \alpha} \frac{1}{|\beta|!} \frac{\partial}{\partial x^\beta}(x^\alpha) P^{(\beta)}(x, D)\phi = P^{(\alpha)}(x, D)\phi.$$

Therefore:

$$(1.3) \qquad P^{(\alpha)}(x, D) = [\boldsymbol{P}, x^\alpha] - \sum_{0 < \beta < \alpha} \frac{1}{|\beta|!} \frac{\partial}{\partial x^\beta}(x^\alpha) P^{(\beta)}(x, D).$$

Similarly, by applying (1.2) this time:

$$(1.4)\quad (-1)^{|\alpha|}\, P_{(\alpha)}(x,D) = [P, D_\alpha] - \sum_{0<\beta<\alpha} \frac{(-1)^{|\beta|}}{|\beta|!} (D_\alpha)^{(\beta)} P_{(\beta)}(x,D).$$

2. The norms $\| \ \|_s$. We consider now the n-dimensional real space R^n with Cartesian coordinates $x^1, \cdots, x^n$; we set $|x| = (|x^1|^2 + \cdots + |x^n|^2)^{\frac{1}{2}}$; $dx = dx^1 \cdots dx^n$. Let us denote by $C_0^\infty(R^n)$ the subset of $C^\infty(R^n)$ consisting of functions with compact support. We define the Fourier transform of $\phi \in C_0^\infty(R^n)$ as

$$\hat{\phi}(\xi) = \int_{R^n} \phi(x) e^{-2i\pi\langle x,\xi\rangle} dx,$$

where ξ belongs to the dual R_n of R^n and $\langle x, \xi\rangle = x^1\xi_1 + \cdots + x^n\xi_n$. The reciprocity formula holds:

$$\phi(x) = \int_{R_n} \hat{\phi}(\xi) e^{2i\pi\langle x,\xi\rangle} d\xi.$$

We set $|\xi| = (|\xi_1|^2 + \cdots + |\xi_n|^2)^{\frac{1}{2}}$. Let s be any real number. We set:

$$\|\phi\|_s = \Big[\int_{R^n} (1 + |\xi|^2)^s\, |\hat{\phi}(\xi)|^2\, d\xi\Big]^{\frac{1}{2}}, \quad \phi \in C_0^\infty(R^n).$$

The norms $\| \ \|_s$ are invariant in the following sense: Let η be an automorphism of the C^∞ structure of R^n; $\phi \to \phi \circ \eta$ is a one-to-one mapping of $C_0^\infty(R^n)$ onto itself. For every compact subset K of R^n there is a constant $C_K < +\infty$ such that, if $\phi \in C_0^\infty(R^n)$ and if support of $\phi \subset K$,

$$\|\phi \circ \eta\|_s \leqq C_K \|\phi\|_s$$

(see Peetre [1], p. 18).

Let us go back to the manifold Ω. For any open subset Ω' of Ω, we denote by $C_0^\infty(\Omega')$ the C^∞ functions in Ω whose supports are compact and contained in Ω'. Assume that Ω' is covered by local coordinates $x^1, \cdots, x^n$ and let J be the diffeomorphism they define from Ω' onto an open subset O' of R^n; then $\phi \to \phi \circ J^{-1}$ is a one-to-one linear map of $C_0^\infty(\Omega')$ onto $C_0^\infty(O')$. We may define the norm $\|\phi\|_s$ of $\phi \in C_0^\infty(\Omega')$ by equating it to $\|\phi \circ J^{-1}\|_s$. Of course $\|\phi\|_s$ depends on the coordinates x^j; but if we change coordinates and denote by $|||\phi|||_s$ the new corresponding norm, to every compact subset K of Ω' corresponds a constant $C_K < +\infty$ such that

$$C_K^{-1} \|\phi\|_s \leqq |||\phi|||_s \leqq C_K \|\phi\|_s$$

provided that the support of ϕ lies in K. This is a consequence of the invariance of the norms $\| \ \|_s$ in R^n we have indicated above.

Let now K be an arbitrary compact set in Ω. We may construct a partition of unity $\alpha_1, \cdots, \alpha_m$ in $C_0^\infty(\Omega)$ over some neighborhood of K such that the support of each α_j lies in some local map Ω'_j. In Ω'_j we may define the norms $\| \ \|_s$ and then, for $\phi \in C^\infty(\Omega)$ with support in K, we may set;

$$\| \phi \|_s = \{ \| \alpha_1 \phi \|_s^2 + \cdots + \| \alpha_m \phi \|_s^2 \}^{\frac{1}{2}}.$$

If one changes the partition of unity or the local coordinates, one gets an equivalent norm. Anyway, let C_K^∞ be the set of $\phi \in C_0^\infty(\Omega)$ having their support in K. The completion of C_K^∞ for the norm $\| \phi \|_s$ is denoted by H^s_K; H^s_K is a Hilbert space (but the Hilbert structure depends on the partition of unity $\{\alpha_j\}$ and on the local coordinates[2]).

Let us assume that we have used the same partition of unity and the same local coordinates in defining H^s_K whatever be s real. Then we can state the following properties:

1) The identity mapping of C_K^∞ can be extended, when $s \geqq t$, as a one-to-one continuous linear map $H^s_K \to H^t_K$, in fact of norm $\leqq 1$, which we shall call the natural embedding of H^s_K into H^t_K.

LEMMA 1. *If* $s > t$ *and* $s \geqq 0$, *the norm of the natural embedding* $H^s_K \to H^t_K$ *tends to zero when the diameter of* K *tends to zero.*

For the proof, see e. g. Malgrange [1] (Lemma I. 2. 3).

2) Let Q be a differential operator defined and of order $\mu \geqq 0$ on some neighborhood of K. Then, for $\phi \in C_K^\infty$,

$$\| Q\phi \|_s \leqq A_K(s, Q) \| \phi \|_{s+\mu}$$

where $A_K(s, Q) < +\infty$ depends on s, Q, K but not on ϕ. Hence $\phi \to Q\phi$, which maps C_K^∞ into itself, expands as a bounded linear map $H^{s+\mu}_K \to H^s_K$. The case $\mu = 0$ is important: Q is then the multiplication by a C^∞ function ψ on some neighborhood of K and, for $\phi \in C_K^\infty$,

$$\| \psi\phi \|_s \leqq A_K(s, \psi) \| \phi \|_s.$$

All this is valid whatever be s real.

When $\Omega = R^n$, we may define, for s real, the completion H^s of $C_0^\infty = C_0^\infty(R^n)$ for the norm $\phi \to \| \phi \|_s$. We shall make use of different properties of the spaces H^s:

i) for $t \leqq s$, $H^s \subset H^t$; H^s is dense in H^t; the norm of the embedding $H^s \to H^t$ is $\leqq 1$;

---

[2] However, as a topological vector space, H^s_K is invariant.

ii) for $\phi, \psi \in C_0^\infty$, the bilinear functional

$$(\phi, \psi) \to \langle \phi, \psi \rangle = \int_{R^n} \phi(x) \psi(x)\, dx$$

can be extended to $H^s \times H^{-s}$ and turns those spaces into the duals of each other.

Now for a few words about distributions in Ω. The elements of $H^s{}_K$ can be canonically regarded as such distributions, whose supports, morevoer, lie in K. If u is a distribution with compact support K_u, we shall use the notation $u \in H^s$ to indicate that $u \in H^s{}_K$ whatever be K compact, $K \supset K_u$. Similarly, we shall use expressions like: a set of distributions u bounded, compact, etc. in H^s; a net of distributions converging in H^s; etc. This applies only, when Ω is an arbitrary manifold, in our set up, to sets or nets of distributions having all their support in some fixed compact subset K of Ω and means that the properties in question really occur in $H^s{}_K$.

Given any distribution u on Ω and any $\phi \in C_0^\infty(\Omega)$, there is a real number s such that $\phi u \in H^s$. In general, s depends on ϕ. If s can be taken independently of ϕ, we say that $u \in H^s{}_{\text{loc}}(\Omega)$. In other words, given any distribution v in Ω and any open set $\Omega' \subset \Omega$, $\overline{\Omega'}$ compact, there is a real q such that the restriction of v to Ω' belongs to $H^q{}_{\text{loc}}(\Omega')$. If $u \in H^s{}_{\text{loc}}(\Omega)$ whatever be s real, u is a C^∞ function on Ω.

Let us finally add that all the differential operators will be assumed, in the sequel, to act in the sense of distributions.

3. Some lemmas. Let now ρ be a C_0^∞ function on R^n, $\int_{R^n} \rho(x)\, dx = 1$. For $t > 0$, we set: $\rho_t(x) = \frac{1}{t^n} \rho(\frac{x}{t})$. The Fourier transform of ρ_t is

$$(\rho_t)^\wedge(y) = \int_{R^n} e^{-2i\pi\langle x, y\rangle} \rho(\frac{x}{t}) \frac{dx}{t^n} = \hat{\rho}(ty).$$

Lemma 2. *For every real number μ' there is a number $\mu \geqq 0$ such that, for all multi-indices $\beta = (\beta_1, \cdots, \beta_r)$, $1 \leqq \beta_j \leqq n$ for $j = 1, \cdots, r$, such that $|\beta| \geqq \mu$, we have, for all numbers $0 < t < 1$,*

$$\| x^\beta \rho_t \|_{\mu'} \leqq C(|\beta|)$$

where $C(|\beta|) < +\infty$ depends only on ρ and $|\beta|$.

Let $\mu'' = \sup(\mu', 0)$.

$$\begin{aligned} \| x^\beta \rho_t \|^2{}_{\mu'} &\leqq \int (1 + |y|^2)^{\mu''} |(D_\beta)_y \hat{\rho}(ty)|^2\, dy \\ &= t^{2|\beta|} \int (1 + |y|^2)^{\mu''} |(D_\beta \hat{\rho})(ty)|^2\, dy \\ &\leqq t^{2|\beta| - 2\mu''} \int (1 + |ty|^2)^{\mu''} |(D_\beta \hat{\rho})(ty)|^2\, dy \\ &= t^{2|\beta| - 2\mu'' - n} \int (1 + |\xi|^2)^{\mu''} |D_\beta \hat{\rho}(\xi)|^2\, d\xi \end{aligned}$$

and therefore any $\mu \geqq \mu'' + \frac{n}{2}$ has the desired property.

For $\psi \in C_0^\infty$, we set:

$$\| \psi \|_{\sigma,\infty} = \sup_{\xi \in R_n} (1 + | \xi |^2)^{\sigma/2} | \hat{\psi}(\xi) |, \ \sigma \text{ real.}$$

If $\phi \in C_0^\infty$ also, then:

$$(3.1) \qquad \| \phi * \psi \|_\sigma \leqq \| \phi \|_{\sigma'} \| \psi \|_{\sigma'', \infty}$$

whatever be the real numbers σ', σ'' such that $\sigma' + \sigma'' = \sigma$.

LEMMA 3. *Let β be a multi-index: $\beta = (\beta_1, \cdots, \beta_r)$, $1 \leqq \beta_j \leqq n$ for $j = 1, \cdots, r$. Whatever be $0 < t < 1$,*

$$\| x^\beta \rho_t \|_{|\beta|, \infty} \leqq C(| \beta |)$$

where $C(| \beta |) < +\infty$ depends only on ρ and $| \beta |$.

We have:

$$\begin{aligned} \sup_{y \in R_n, 0<t<1} & (1 + | y |^2)^{|\beta|/2} | (D_\beta)_y \hat{\rho}_t(y) | \\ &= \sup_{y \in R_n, 0<t<1} t^{|\beta|} (1 + | y |^2)^{|\beta|/2} | (D_\beta \hat{\rho})(ty) | \\ &\leqq \sup_{y \in R_n, 0<t<1} (1 + | ty |^2)^{|\beta|/2} | (D_\beta \hat{\rho})(ty) | \\ &= \sup_{\xi \in R_n} (1 + | \xi |^2)^{|\beta|/2} | (D_\beta \hat{\rho})(\xi) | < +\infty \end{aligned}$$

(the Fourier transform of a C_0^∞ function decreases, as well as each one of its derivatives, when $| \xi | \to +\infty$, faster than any power of $\frac{1}{| \xi |}$).

COROLLARY. *Let σ be any real number. Whatever be $0 < t < 1$ and $\phi \in C_0^\infty$,*

$$\| (x^\beta \rho_t) * \phi \|_\sigma \leqq C(| \beta |) \| \phi \|_{\sigma - |\beta|}.$$

Immediate consequence of Formula (3.1) and Lemma 3.

LEMMA 4. *Let O be an open set in R^n, $R(x;y)$ a C^∞ function in $O \times O$ whose derivatives, up to the order $k-1$ included ($k \geqq 1$), vanish on the diagonal $x = y$. Then one may write*

$$R(x;y) = \sum_{|\alpha|=k} (x-y)^\alpha R_\alpha(x;y)$$

where the $R_\alpha(x,y)$ are C^∞ functions in $O \times O$.

We recall that $(x-y)^\alpha = (x^{\alpha_1} - y^{\alpha_1}) \cdots (x^{\alpha_r} - y^{\alpha_r})$ where $1 \leqq \alpha_j \leqq n$

for $j = 1, \cdots, r$; $\alpha = (\alpha_1, \cdots, \alpha_r)$. It is enough to prove the Lemma for $k = 1$; by iteration, one gets it then for arbitrary k. Let us therefore assume that $R(x;y) = 0$ if $x = y$. For $j = 1, \cdots, n$, let us set:

$$R_j(x;y) = \frac{1}{x^j - y^j}\{R(x^1, \cdots, x^j, y^{j+1}, \cdots, y^n; y^1, \cdots, y^n) \\ - R(x^1, \cdots, x^{j-1}, y^j, \cdots, y^n; y^1, \cdots, y^n)\}.$$

Since $R(y^1, \cdots, y^n; y^1, \cdots, y^n) = 0$, we have

$$R(x;y) = \sum_{j=1}^{n} (x^j - y^j) R_j(x;y).$$

We have to show that the $R_j(x;y)$ are C^∞ in $O \times O$. But it is enough to show it when $n = 1$, in which case the result is trivial.

Let $K(x,u)$ be a C_0^∞ function on $R_x^n \times R_u^n$. We set:

$$[\phi \underset{K}{\otimes} \psi](x) = \int_{R^n} \phi(x-u) K(x,u) \psi(u)\, du,$$

where $\phi, \psi \in C^\infty = C^\infty(R^n)$.

LEMMA 5. *Let σ, τ be two real numbers. For every $\phi, \psi \in C_0^\infty$,*

$$\| \phi \underset{K}{\otimes} \psi \|_{\sigma+\tau} \leq C(K;\sigma,\tau) \| \phi \|_\sigma \| \psi \|_\tau ;$$

$C(K;\sigma,\tau)$ is a constant $< +\infty$ depending on K, σ, τ but not on ϕ, ψ.

Of course, $C_0^\infty = C_0^\infty(R^n)$. We set $s = \sigma + \tau$.

We may write $K(x,y) = \int e^{2i\pi(\langle x,y\rangle + \langle u,v\rangle)} \hat{K}(y,v)\, dy dv$, where $\hat{K}(y,v)$ is a function belonging to $\mathcal{S}_{y,v}$.* In particular, whatever be the integer $k \geqq 0$ the function $(1 + |y| + |v|)^k \hat{K}(y,v)$ is square integrable in $R_y^n \times R_v^n$. Let us set

$$H(x,y,v) = \int e^{2i\pi(\langle x,y\rangle + \langle u,v\rangle)} \phi(x-u) \psi(u)\, du.$$

We have:

$$[\phi \underset{K}{\otimes} \psi](x) = \int \hat{K}(y,v) H(x,y,v)\, dy dv. \tag{3.2}$$

It is obvious that $H(x,y,v)$ is C^∞ in x, y, v, and, regarded as a function of x, has its support in a fixed compact set independent of y, v. On the other hand, $H(x,y,v)$ is bounded in R^{3n}. From this follows that the Fourier transform of the right hand side of (3.2) equals

$$\int \hat{K}(y,v) \hat{H}(\xi,y,v)\, dy dv,$$

---

* $\mathcal{S}_w$ is the space of C^∞ functions of $w \in R^M$ decreasing at infinity, as well as each one of their derivatives, faster than any power of $1/|w|$.

where $\hat{H}(\xi, y, v)$ is the Fourier transform of $H(x, y, v)$ with respect to x. We have then, in view of Schwarz inequality,

$$(3.3)\quad (1+|\xi|^2)^s|(\phi \underset{K}{\otimes} \psi)\hat{\ }(\xi)|^2 \leqq \left(\int (1+|y|+|v|)^k|\hat{K}(y,v)|^2\, dydv\right)$$
$$\times \left(\int (1+|y|+|v|)^{-k}(1+|\xi|^2)^s|\hat{H}(\xi,y,v)|^2\, dydv\right),$$

where k is any integer $\geqq 0$. We shall show now that under the hypotheses of Lemma 5, there is an integer $N \geqq 0$ such that, for all $y, v \in R_n$,

$$\int (1+|\xi|^2)^s|\hat{H}(\xi,y,v)|^2\, d\xi \leqq C(1+|y|+|v|)^N \|\phi\|^2_\sigma \|\psi\|^3_\tau.$$

Choosing then $k > N+2n$ and integrating with respect to ξ both sides of (3.3), we obtain the lemma.

We have $\hat{H}(\xi, y, v) = \hat{\phi}(\xi - y)\hat{\psi}(\xi - y - v)$. Let us now use the fact that for every real number r there is a finite constant C_r such that for all $\xi, \eta \in R_n$,

$$(1+|\xi|^2)^r \leqq C_r(1+|\eta|^2)^{|r|}(1+|\xi-\eta|^2)^r.$$

We get:

$$(1+|\xi|^2)^s|\hat{H}(\xi,y,v)|^2 \leqq C(1+|y|^2)^{|\sigma|}(1+|y+v|^2)^{|\tau|}$$
$$\times(1+|\xi-y|^2)^\sigma|\hat{\phi}(\xi-y)|^2(1+|\xi-y-v|^2)^\tau|\hat{\psi}(\xi-y-v)|^2.$$

By integrating the two sides of this inequality, we get

$$\int (1+|\xi|^2)^s|\hat{H}(\xi,y,v)|^2\, d\xi \leqq C_1(1+|y|+|v|)^{2(|\sigma|+|\tau|)}$$
$$\times \sup_{\xi \in R_n}(1+|\xi|^2)^\tau|\hat{\psi}(\xi)|^2 \cdot \|\phi\|^2_\sigma.$$

At that point it should be noted that since $K(x, u)$ has its support in a fixed compact subset of $R_x^n \times R_u^n$, we may as well assume that the support of ψ lies in a fixed compact set $\mathcal{K}$. Let $\alpha \in C_0^\infty(R^n)$, $\alpha \equiv 1$ on $\mathcal{K}$. We have $\hat{\psi} = \hat{\psi} * \hat{\alpha}$ and therefore

$$(1+|\xi|^2)^{\tau/2}|\hat{\psi}(\xi)| \leqq C\int (1+|\eta|^2)^{|\tau|/2}|\hat{\alpha}(\eta)|$$
$$\times(1+|\xi-\eta|^2)^{\tau/2}|\hat{\psi}(\xi-\eta)|\, d\eta \leqq C_2\|\psi\|_\tau,$$

by applying Schwarz inequality. This concludes the proof of Lemma 5.

4. Statement of the main result. Let Ω be an n-dimensional C^∞ manifold.

In order to abbreviate the forthcoming statements, we shall *constantly* make use of the following convention.

Let $\boldsymbol{R}$, $\boldsymbol{S}$ be two differential operators defined near a point ω of Ω (i.e. on some open neighborhood of ω). We shall make statements of the following kind:

The inequality $\| R\phi \|_r \leqq C \| S\phi \|_s$ *is valid at* ω.

The meaning of it is the following:

Let Ω' be an open neighborhood of ω on which both $\boldsymbol{R}$ and $\boldsymbol{S}$ are defined.

i) There is an open neighborhood $U \subset \Omega'$, depending on $\boldsymbol{R}$, $\boldsymbol{S}$, r, s and the local coordinates near ω used to define the norms $\| \ \|_\sigma$,

ii) there is a finite constant C, depending on $\boldsymbol{R}$, $\boldsymbol{S}$, r, s and the local coordinates, such that, for every $\phi \in C_0^\infty(\Omega)$ with support in U,

$$\| \boldsymbol{R}\phi \|_r \leqq C \| \boldsymbol{S}\phi \|_s.$$

Of course C is independent of ϕ; we shall handle C as a kind of general symbol.

In order to state the main result of this article, we shall introduce the following definition:

Let $\omega \in \Omega$, $\boldsymbol{P}$ be a differential operator defined on Ω. We shall always denote by m the order of $\boldsymbol{P}$ on some open subset of Ω containing ω.

Let σ, a, b be real numbers. Let us consider the following properties which may be valid at the point ω of Ω:

(A_σ) $$\| \phi \|_{\sigma+a} \leqq C \| \boldsymbol{P}\phi \|_\sigma.$$

(B_σ) *Whatever be the differential operator* $\boldsymbol{L}$ *defined and of order* $\mu \leqq 1$ *near* ω,

$$\| [\boldsymbol{P}, \boldsymbol{L}]\phi \|_{\sigma+b} \leqq C \| \boldsymbol{P}\phi \|_{\sigma+\mu}.$$

DEFINITION 1. *We say that* $\boldsymbol{P}$ *is regular at* ω *if there are numbers* σ_0 *real,* a *real,* $b > 0$ *such that* (A_σ), (B_σ) *hold at* ω *for every* $\sigma \geqq \sigma_0$.

We say that $\boldsymbol{P}$ is regular in some open subset Ω_0 of Ω if $\boldsymbol{P}$ is regular at every point ω of Ω_0 (σ_0, a, b will then generally depend on the point ω).

Remark 4.1. If (A_σ) is valid at ω, a must necessarily be $\leqq m$; $a = m$ if and only if $\boldsymbol{P}$ is elliptic in some neighborhood of ω.

If (B_σ) holds at ω, b must be $\leqq 1$ and $b = 1$ if and only if $\boldsymbol{P}$ is elliptic near ω.

Our main theorem will then be:

THEOREM 1. *If* $\boldsymbol{P}$ *is regular in* Ω, $\boldsymbol{P}$ *is hypoelliptic in* Ω.

We shall prove a slightly more precise statement:

THEOREM 1′. *Let* $\boldsymbol{P}$ *be regular in* Ω; *let* Ω_1 *be an open subset of* Ω *with compact closure. There is a real number* a_1 *such that, whatever be* s *real and the distribution* u *on* Ω,

$$\boldsymbol{P}u \in H^s_{\mathrm{loc}}(\Omega_1) \text{ implies } u \in H^{s+a_1}_{\mathrm{loc}}(\Omega_1).$$

5. First consequences of (A_σ), (B_σ). Let us introduce the following property, which may be valid at $\omega \in \Omega$:

$(B_s)_M{}^{\#}$ *Whatever be the* $\lambda \leqq M$ *differential operators* $\boldsymbol{L}_1, \cdots, \boldsymbol{L}_\lambda$ *of respective orders* $d_1 \leqq 1, \cdots, d_\lambda \leqq 1$ *near* ω,

$$\| [\cdots [\boldsymbol{P}, \boldsymbol{L}_1], \cdots \boldsymbol{L}_\lambda] \phi \|_{s-d+b} \leqq C \| \boldsymbol{P}\phi \|_s$$

with $d = d_1 + \cdots + d_\lambda$.

LEMMA 6. *Assume that* (B_s) *holds at* ω, *with* $b \geqq 0$, *for* $s = \sigma$, $\sigma + 1, \cdots, \sigma + M$ $(M \geqq 1)$. *Then* $(B_{\sigma+M})_M{}^{\#}$ *holds at* ω.

Let us set $\boldsymbol{R}_\lambda = [\cdots [\boldsymbol{P}, \boldsymbol{L}_1], \cdots \boldsymbol{L}_\lambda]$. We are going to show that

$$\| \boldsymbol{R}_\lambda \phi \|_{s-d+b} \leqq C \| \boldsymbol{P}\phi \|_s \text{ at } \omega \tag{5.1}$$

for $s = \sigma + \lambda$, $\sigma + \lambda + 1, \cdots, \sigma + M$. For $\lambda = M$, this will be exactly what we want.

We reason by induction on λ. When $\lambda = 1$, (5.1) is a trivial consequence of the validity of (B_s) for $s = \sigma, \sigma + 1, \cdots, \sigma + M$. We assume $\lambda \geqq 2$ and that (5.1) is valid up to $\lambda - 1$. We have $\boldsymbol{R}_\lambda = [\boldsymbol{R}_{\lambda-1}, \boldsymbol{L}_\lambda]$ and therefore, at ω, setting $d' = d_1 + \cdots + d_{\lambda-1}$:

$$\begin{aligned} \| \boldsymbol{R}_\lambda \phi \|_{s-bd+} &\leqq \| \boldsymbol{R}_{\lambda-1} \boldsymbol{L}_\lambda \phi \|_{s-d_\lambda-d'+b} + \| \boldsymbol{L}_\lambda \boldsymbol{R}_{\lambda-1} \phi \|_{s-d'+b-d_\lambda} \\ &\leqq \| \boldsymbol{R}_{\lambda-1} \boldsymbol{L}_\lambda \phi \|_{s-d_\lambda-d'+b} + C \| \boldsymbol{R}_{\lambda-1} \phi \|_{s-d'+b}. \end{aligned}$$

Assume that s belongs to the set of numbers $\{\sigma + \lambda, \cdots, \sigma + M\}$. Then s and $s - d_\lambda$ (since $d_\lambda \leqq 1$) both belong to the set

$$\{\sigma + \lambda - 1, \cdots, \sigma + M\};$$

hence at ω:

$$\| \boldsymbol{R}_{\lambda-1} \boldsymbol{L}_\lambda \phi \|_{s-d_\lambda-d'+b} \leqq C \| \boldsymbol{P} \boldsymbol{L}_\lambda \phi \|_{s-d_\lambda},$$

$$\| \boldsymbol{R}_{\lambda-1} \phi \|_{s-d'+b} \leqq C \| \boldsymbol{P}\phi \|_s.$$

Since $b \geqq 0$,

$$\begin{aligned} \| \boldsymbol{P} \boldsymbol{L}_\lambda \phi \|_{s-d_\lambda} &\leqq \| \boldsymbol{L}_\lambda \boldsymbol{P} \phi \|_{s-d_\lambda} + \| [\boldsymbol{P}, \boldsymbol{L}_\lambda] \phi \|_{s-d_\lambda} \\ &\leqq C \| \boldsymbol{P}\phi \|_s + \| [\boldsymbol{P}, \boldsymbol{L}_\lambda] \phi \|_{s-d_\lambda+b}. \end{aligned}$$

But certainly $s \in \{\sigma, \cdots, \sigma + M\}$; hence at ω

$$\| [\boldsymbol{P}, \boldsymbol{L}_\lambda] \phi \|_{s-d_\lambda+b} \leqq C \| \boldsymbol{P}\phi \|_s.$$

This concludes the proof.

LEMMA 7. *Assume that* (A_s) *holds at* ω. *Let* M_0 *be the smallest integer* $\geqq 2m - a + b$. *If* $(B_s)_{M_0}{}^{\#}$ *holds at* ω, $(B_s)_M{}^{\#}$ *holds at* ω *whatever be the integer* M.

We keep the same notations as in the proof of Lemma 6. Let $x^1, \cdots, x^n$ be local coordinates near ω. Let $P(x,D)$, $R_\lambda(x,D)$ be the respective expressions of $\boldsymbol{P}$ and $\boldsymbol{R}_\lambda$ in those coordinates. We may write

$$R_\lambda(x,D) = \sum R_{\lambda,\alpha}{}^{\beta}(x,D) P_{(\beta)}{}^{(\alpha)}(x,D),$$

where the $R_{\lambda,\alpha}{}^{\beta}(x,D)$ are differential operators depending on $\boldsymbol{L}_1, \cdots, \boldsymbol{L}_\lambda$. Observe that in the summation, because of the definition of $\boldsymbol{R}_\lambda$, we will always have $|\alpha| \geqq \lambda - d$, $|\alpha| + |\beta| \geqq \lambda$.

Assume $\lambda \geqq M \geqq 2m - a + b$. Then we must have $d \geqq m - a + b$ or else $\boldsymbol{R}_\lambda \equiv 0$ near ω. For if $d < m - a + b$, $|\alpha| \geqq \lambda - d > m$ and $P_{(\beta)}{}^{(\alpha)} \equiv 0$ near ω.

If $d \geqq m - a + b$, $\|\phi\|_{s-d+m+b} \leqq \|\phi\|_{s+a}$.

Observe on the other hand that the order of $\boldsymbol{R}_\lambda$ near ω is $\leqq m$ whatever be λ. Hence at ω

$$\|\boldsymbol{R}_\lambda \phi\|_{s-d+b} \leqq C \|\phi\|_{s-d+m+b}$$

and by combining those two inequalities, we get at ω

$$\|\boldsymbol{R}_\lambda \phi\|_{s-d+b} \leqq C \|\phi\|_{s+a}.$$

Then the Lemma is simply a consequence of (A_s).

If $(B_s)_M{}^\#$ holds at ω whatever be M, we say that $(B_s)^\#$ holds at ω.

LEMMA 8. *Property $(B_s)^\#$ is valid at ω if and only if the following property is valid at ω:*
(C_s) *Whatever be the differential operator $\boldsymbol{Q}$ defined and of order μ near ω,*

$$\|[\boldsymbol{P},\boldsymbol{Q}]\phi\|_{s-\mu+b} \leqq C \|\boldsymbol{P}\phi\|_s.$$

1) $\underline{(B_s)^\# \Longrightarrow (C_s)}$

Let us use again the local coordinates x^j; let $Q(x,D)$ be the expression of $\boldsymbol{Q}$ in those coordinates. According to Formula (1.0) we have at ω:

$$\|[\boldsymbol{P},\boldsymbol{Q}]\phi\|_{s-\mu+b} \leqq C \sum_{|\beta|+|\gamma|>0} \|P_{(\gamma)}{}^{(\beta)}(x,D)\phi\|_{s-|\gamma|+b},$$

since the order of $Q_{(\beta)}{}^{(\gamma)}(x,D)$ near ω is $\leqq \mu - |\gamma|$.

Observe that if $1 \leqq \lambda \leqq n$, $1 \leqq \lambda' \leqq n$,

$$[[\boldsymbol{P}, x^\lambda], \frac{\partial}{\partial x^{\lambda'}}] = [[\boldsymbol{P}, \frac{\partial}{\partial x^{\lambda'}}], x^\lambda]$$

and therefore $P_{(\gamma)}{}^{(\beta)}(x,D)$ is the expression in the coordinates x^j of

$$[\cdots[\cdots[[\boldsymbol{P},x^{\beta_1}],\cdots x^{\beta_r}],\frac{\partial}{\partial x^{\gamma_1}}],\cdots\frac{\partial}{\partial x^{\gamma_s}}]$$

assuming that $\beta=(\beta_1,\cdots,\beta_r)$, $\gamma=(\gamma_1,\cdots,\gamma_s)$. Then, from $(B_s)^\#$, it follows immediately that, at ω

$$\| P_{(\gamma)}{}^{(\beta)}(x,D)\phi \|_{s-|\gamma|+b} \leqq C \| \boldsymbol{P}\phi \|_s.$$

2) $\underline{(C_s) \Longrightarrow (B_s)^\#}$

It is easily seen that $[\cdots[\boldsymbol{P},\boldsymbol{L}_1],\cdots\boldsymbol{L}_\lambda]$ is a sum of terms of the form

$$\pm \boldsymbol{L}_{i_1}\cdots\boldsymbol{L}_{i_\alpha}[\boldsymbol{P},\boldsymbol{L}_{j_1}\cdots\boldsymbol{L}_{j_\beta}]$$

where $(i_1,\cdots,i_\alpha,j_1,\cdots,j_\beta)$ is simply a permutation of $(1,2,\cdots,\lambda)$. We have at ω:

$$\begin{aligned}&\| \boldsymbol{L}_{i_1}\cdots\boldsymbol{L}_{i_\alpha}[\boldsymbol{P},\boldsymbol{L}_{j_1}\cdots\boldsymbol{L}_{j_\beta}]\phi \|_{s-d+b}\\ &\qquad \leqq C \| \boldsymbol{P},\boldsymbol{L}_{j_1}\cdots\boldsymbol{L}_{j_\beta}]\phi \|_{s-d^0+b} \leqq C' \| \boldsymbol{P}\phi \|_s,\end{aligned}$$

where $d=d_1+\cdots+d_\lambda$, $d^0=d_{j_1}+\cdots+d_{j_\beta}$; $\boldsymbol{L}_{j_1}\cdots\boldsymbol{L}_{j_\beta}$ is precisely a differential operator of order d^0 near ω.

COROLLARY. *Let $x^1,\cdots,x^n$ be local coordinates near ω, $P(x,D)$ the expression of $\boldsymbol{P}$ in those coordinates.*

If (C_s) is true at ω, then whatever be the multi-indices α,β, $|\alpha|+|\beta|>0$,

$$\| P_{(\beta)}{}^{(\alpha)}(x,D)\phi \|_{s-|\beta|+b} \leqq C \| \boldsymbol{P}\phi \|_s$$

holds at ω.

The important result in this section is the following:

LEMMA 9. *Assume that (A_σ), (B_σ) hold at ω, with $b \geqq 0$, for every $\sigma \geqq \sigma_0$. Let M_0 be the smallest integer $\geqq 2m-a+b$. Let $s_0=\sigma_0+M_0$.*

Then (C_s) holds at ω for every $s \geqq s_0$.

Lemma 6 tells us that $(B_{\sigma'})$, valid at ω for $\sigma \leqq \sigma' \leqq \sigma+M_0$, implies $(B_{\sigma+M_0})_{M_0}{}^\#$ at ω.

Lemma 7 tells us that $(B_{\sigma+M_0})_{M_0}{}^\# \Longrightarrow (B_{\sigma+M_0})^\#$ provided that $(A_{\sigma+M_0})$ is true at ω.

Lemma 8 state that $(B_{\sigma+M_0})^\#$ is equivalent with $(C_{\sigma+M_0})$.

Q. E. D.

Remark 5.1. From now on, instead of working on the basis that (A_σ) and (B_σ) are valid at ω for $\sigma \geqq \sigma_0$, we shall assume that (A_s) and (C_s) are valid at ω for $s \geqq s_0$.

We conclude this section with a trivial result that is going to be needed later on.

LEMMA 10. *Assume that* (C_s) *holds at* ω. *Let* Ω' *be some open set containing* ω. *There is an open neighborhood* $\Omega_s'' \subset \Omega'$ *of* ω *such that for every* $\psi \in C^\infty(\Omega')$ *and every* $\phi \in C_0^\infty(\Omega''_s)$,

$$\| [\boldsymbol{P}, \psi] \phi \|_{s+b} \leqq C \| \boldsymbol{P} \phi \|_s$$

This means that the inequality in the Lemma is valid for $\phi \in C_0^\infty(\Omega)$ having its support in a neighborhood of ω independent of ψ.

Proof. Let $x^1, \cdots, x^n$ be a system of coordinates covering an open neighborhood $\Omega_1' \subset \Omega'$ of ω; let $P(x, D)$ be the expression of $\boldsymbol{P}$ in those coordinates. If $\phi \in C_0^\infty(\Omega_1')$, we have, according to Formula (1.1):

$$\| [\boldsymbol{P}, \psi] \phi \|_{s+b} \leqq C \sum_{|\beta|>0} \| P^{(\beta)}(x, D) \phi \|_{s+b}$$

(in fact, we have to assume something like $\overline{\Omega_1'}$ compact, $\overline{\Omega_1'} \subset \Omega'$). For every multi-index β, $|\beta| > 0$, we have according to the Corollary of Lemma 8,

$$\| P^{(\beta)}(x, D) \phi \|_{s+b} \leqq C \| \boldsymbol{P} \phi \|_s$$

for $\phi \in C_0^\infty(\Omega'_{(\beta)})$, where $\Omega'_{(\beta)}$ is a suitable neighborhood of ω. Observe that $P^{(\beta)}(x, D) \equiv 0$ near ω for $|\beta| > m$. We may take then

$$\Omega''_s = \Omega'_1 \cap \bigcap_{0<|\beta|\leqq m} \Omega'_{(\beta)}.$$

6. Properties (A_s), (C_s) and Friedrichs mollifiers.

We choose local coordinates $x^1, \cdots, x^n$ near ω; we shall always assume that $x^1(\omega) = \cdots = x^n(\omega) = 0$. The norms $\| \;\; \|_s$ are computed by means of those coordinates; $P(x, D)$ will be the expression of $\boldsymbol{P}$ in the x^j.

Let ρ be a C_0^∞ function on R^n, $\int_{R^n} \rho(x)\, dx = +1$. For $t > 0$, we set:

$$\rho_t(x) = t^{-n} \rho(x/t).$$

Let J be the homeomorphism $\omega' \to (x^1(\omega'), \cdots, x^n(\omega'))$ of a neighborhood Ω' of ω onto an open neighborhood O' of the origin $0 \in R^n$; $J(\omega) = 0$. The map $\phi \to \phi \circ J^{-1}$ is *one-to-one* from $C_0^\infty(\Omega')$ *onto* $C_0^\infty(O')$. Let $\Omega'' \subset \Omega'$ be open, $\overline{\Omega''}$ compact, $\overline{\Omega''} \subset \Omega'$. We may find $t_0 > 0$ small enough so that $t \leqq t_0$ implies, for $\phi \in C_0^\infty(\Omega'')$, that the support of

$$[\rho_{t*}(\phi \circ J^{-1})](x) = \int_{R^n} \rho_t(x - x')\phi(J^{-1}x')\,dx'$$

lies in O'. Therefore the support of $[\rho_{t*}(\phi \circ J^{-1})] \circ J$ will lie in Ω'.

We still denote by ρ_{t*} the operator $C_0^\infty(\Omega'') \to C_0^\infty(\Omega')$

$$\phi \to [\rho_{t*}(\phi \circ J^{-1}| \circ J.$$

This operator ρ_{t*} can be extended as a linear operator from the space of distributions in Ω, with compact support contained in Ω'', into $C_0^\infty(\Omega')$. In particular (and that is what we are going to need later on), if $u \in H^s{}_K$, K compact, $K \subset \Omega''$, $\rho_{t*}u$ is a C_0^∞ function (with support in Ω'). Moreover, when $t > 0$ tends to 0, $\rho_{t*}u \to u$ in the sense of H^s.

From now on we assume that the number t_0 defined above equals 1. We may always be in that case by just replacing $\rho(x)$ by $t_0^{-n}\rho(x/t_0)$.

LEMMA 11. *Assume that* $(A\sigma)$, $(C\sigma)$ *hold at* ω. *Then*

$$\| [\boldsymbol{P}, \rho_{t*}]\phi \|_{\sigma+b} \leqq C \| \boldsymbol{P}\phi \|_\sigma$$

holds at ω *independently of* $0 < t < 1$.

By "independently of t" we mean the following: i) the constant $C < +\infty$ does not depend on t; ii) we may take an open neighborhood N of ω, independent of t, such that the inequality is true for every $\phi \in C_0^\infty(N)$. Here, of course, both C and N depend (in general) on the function ρ.

Proof. According to Lemma 4, we may write, for some integer $\mu \geqq 1$,

$$P(x, D) = \sum_{|\beta| < \mu} \frac{(x-u)^\beta}{|\beta|!} P_{(\beta)}(u, D_x) + \sum_{|\beta| = \mu} (x-u)^\beta R_\beta(x, u, D_x)$$

where the $R_\beta(x, u, D_x)$ are differential operators on O'. The coefficients of $R_\beta(x, u, D_x)$ are C^∞ functions of $(x, u) \in O' \times O'$; the order of $R_\beta(x, u, D_x)$ is $\leqq m$.

If O'' = image of Ω'' under J and $\psi \in C_0^\infty(O'')$, we have:

$$P(x, D)(\rho_{t*}\psi) = P(x, D_x) \int \rho_t(x-u)\psi(u)\,du$$
$$= \sum_{|\beta| < \mu} \frac{1}{|\beta|!} (x^\beta \rho_t)_* P_{(\beta)}(x, D_x)\psi + \sum_{|\beta| = \mu} \int (x-u)^\beta \rho_t(x-u) R_\beta(x, u, D_u)\psi(u)\,du.$$

We have taken into account the fact that

$$Q(D_x)(\rho_t * \psi) = \int \rho_t(x-u)\,Q(D_u)\psi(u)\,du,$$

where $Q(D)$ stands for any polynomial (with constant coefficients!) in $\frac{\partial}{\partial x^1}, \cdots, \frac{\partial}{\partial x^n}$.

According to the Corollary of Lemma 3,

$$\| (x^\beta \rho_t) * P_{(\beta)}(x,D)\psi \|_{\sigma+b} \leqq C \| P_{(\beta)}(x,D)\psi \|_{\sigma+b-|\beta|}$$

independently of t. Let us apply then the corollary of Lemma 8. For $|\beta| > 0$, we have at ω:

$$\| P_{(\beta)}(x,D)\phi \|_{\sigma+b-|\beta|} \leqq C \| P\phi \|_\sigma$$

where $\phi = \psi \circ J$.[8] We are therefore left with the estimation of the norm $\| g \|_{\sigma+b}$ of the function

$$g(x) = \sum_{|\beta|=\mu} \int (x-u)^\beta \rho_t(x-\widehat{u})\,R_\beta(x,u,D_u)\psi(u)\,du,$$

which is a sum of terms of the form

$$g^\alpha(x) = \int (x-u)^\beta \rho_t(x-u)\,R_\beta{}^\alpha(x,u)\,(D_\alpha\psi)(u)\,du.$$

There is a compact set $H \subset R^n$, such that $O'' + H \subset O'$ and that the supports, in $R_x{}^n \times R_u{}^n$, of the functions $\rho_t(x-u)(D_\alpha\psi)(u)$ (whatever be α and $0 < t < 1$) are contained in $(O''+H) \times O''$. Hence we may assume that the functions $R_\beta{}^\alpha(x,u)$ have their supports contained in a fixed compact subset of $R_x{}^n \times R_u{}^n$. This allows to apply Lemma 5:

$$\| g^\alpha \|_{\sigma+b} \leqq C \| x^\beta \rho_t \|_{\mu'} \| D_\alpha \psi \|_{\sigma+b-\mu'}$$

where μ' is any real number (of course, C depends on μ'). On the other hand,

$$\| D_\alpha \psi \|_{\sigma+b-\mu'} \leqq C \| \psi \|_{\sigma+m+b-\mu'}.$$

We choose $\mu' = m - a + b$. According to Property (A_σ):

$$\| \phi \|_{\sigma+m+b-\mu'} = \| \phi \|_{\sigma+a} \leqq C \| \boldsymbol{P}\phi \|_\sigma \ at\ \omega,$$

where $\phi = \psi \circ J$.

---

[8] $P_{(\beta)}(x,D)$ is a differential operator on the open subset O of R^n. Through the diffeomorphism J, it defines a differential operator on $\Omega' \subset \Omega$ whose expression, in the coordi- $x^1, \cdots, x^n$, is $P_{(\beta)}(x,D)$.

Ultimately, we must show that we can choose the integer μ in such a way that the numbers $\| x^{\beta}\rho_t \|_{\mu'}$, $|\beta| = \mu$, are bounded independently of t. This follows from Lemma 2.

Remark 6.1. No assumption whatsoever has been made upon the sign of b: we did not need $b > 0$ or even $b \geqq 0$; b could be any real number.

7. The last lemma. In this section and the next one, we assume that $\boldsymbol{P}$ has properties (A_s) and (C_s) at ω, with $b > 0$ and for every $s \geqq s_0$ (s_0 being some real number). We recall that those properties are:

(A_s) $\quad \| \phi \|_{s+a} \leqq C \| \boldsymbol{P}\phi \|_s.$

(C_s) *Whatever be the differential operator* $\boldsymbol{Q}$ *of order* μ *near* ω,

$$\| [\boldsymbol{P}, \boldsymbol{Q}]\phi \|_{s-\mu+b} \leqq C \| \boldsymbol{P}\phi \|_s.$$

It is essential that a real and $b > 0$ should be independent of $s \geqq s_0$.

The three numbers s_0, a, b give, in some sense, a "measure" of the regularity of $\boldsymbol{P}$ near ω. They will serve to determine the number a_1 of Theorem 1′ and some other regularity properties of $\boldsymbol{P}$—as we are going to see. In view of those properties, let us say that a and b should be as large as possible while s_0 should be as *small* as possible. We recall however that a cannot exceed m and b cannot exceed 1 (Remark 4.1). We shall actually use those facts.

Anyway, in order to abbreviate the forthcoming statements, we shall say that, under our assumption, $\boldsymbol{P}$ *is of type* (s_0, a, b) *at* ω.

Let $x^1, \cdots, x^n$ be local coordinates near ω. We introduce the operator

$$U_p = \left(1 - \frac{\Delta}{4\pi^2}\right)^p, \quad p\text{: integer} \geqq 0.$$

$\Delta = \left(\frac{\partial}{\partial x^1}\right)^2 + \cdots + \left(\frac{\partial}{\partial x^n}\right)^2$; U_p is defined on some open set containing ω.

LEMMA 12. *If* $\boldsymbol{P}$ *is regular at* ω, *so is* $\boldsymbol{P}U_p$. *More precisely, if* $\boldsymbol{P}$ *is of type* (s_0, a, b), $\boldsymbol{P}U_p$ *is of type* $(s_0^+ - 2p + b, a + 2p, b)$ *at* ω, *with* $s_0^+ = \sup(s_0, 0)$.

Let $\sigma \geqq s_0^+$. We have at ω:

$$\begin{aligned} \| \boldsymbol{P}U_p\phi \|_{\sigma-2p+b} &\geqq \| U_p\boldsymbol{P}\phi \|_{\sigma-2p+b} - \| [\boldsymbol{P}, U_p]\phi \|_{\sigma-2p+b} \\ &\geqq \| \boldsymbol{P}\phi \|_{\sigma+b} - C \| \boldsymbol{P}\phi \|_{\sigma}. \end{aligned}$$

Since $\sigma \geqq 0$, $b > 0$, we may apply Lemma 1: if the support of ϕ lies in a suitable neighborhood of ω,

$$C \,\| \boldsymbol{P}\phi \|_{\sigma} \leqq \tfrac{1}{2} \,\| \boldsymbol{P}\phi \|_{\sigma+b}.$$

Therefore, at ω:

$$\| \boldsymbol{P}\phi \|_{\sigma+b} \leqq C \,\| \boldsymbol{P}\boldsymbol{U}_p\phi \|_{\sigma-2p+b}. \tag{7.1}$$

Let us prove first (A_s) for $\boldsymbol{P}\boldsymbol{U}_p$ and $s \geqq s_0{}^{+} - 2p + b$ (moreover, with $a + 2$ instead of a). We have at ω, for $\sigma \geqq s_0$:

$$\| \phi \|_{\sigma+b+a} \leqq C \,\| \boldsymbol{P}\phi \|_{\sigma+b} \quad (\text{since } b \geqq 0).$$

By applying (7.1) and setting $\sigma = s + 2p - b$, we get at ω:

$$\| \phi \|_{s+(a+2p)} \leqq C \,\| \boldsymbol{P}\boldsymbol{U}_p\phi \|_{s}$$

which is what we wanted.

Let us prove now (C_s) for $\boldsymbol{P}\boldsymbol{U}_p$ and $s \geqq s_0{}^{+} - 2p + b$. Let $\boldsymbol{Q}$ be any differential operator of order μ near ω. We have

$$[\boldsymbol{P}\boldsymbol{U}_p, \boldsymbol{Q}] = [\boldsymbol{P}, U_p\boldsymbol{Q}] + \boldsymbol{Q}[U_p, \boldsymbol{P}] + [U_p, \boldsymbol{Q}]\boldsymbol{P}.$$

Note that $[U_p, \boldsymbol{Q}]$ is a differential operator of order $\leqq 2p + \mu - 1$ near ω. Hence we have at ω:

$$\| [\boldsymbol{P}_p, \boldsymbol{Q}]\phi \|_{s-\mu+b} \leqq \| [\boldsymbol{P}, U_p\boldsymbol{Q}]\phi \|_{s-\mu+b} + C(\| [U_p, \boldsymbol{P}]\phi \|_{s+b} + \| \boldsymbol{P}\phi \|_{s+2p});$$

in order to obtain the last term of the left hand side, we have used the fact that $b \leqq 1$.

Let us take $s = \sigma - 2p + b$, $\sigma \geqq s_0{}^{+}$. The order of $U_p\boldsymbol{Q}$ near ω being $2p + \mu$, we have at ω, because of (C_σ) for $\boldsymbol{P}$:

$$\| [\boldsymbol{P}, U_p\boldsymbol{Q}]\phi \|_{\sigma+b-(2p+\mu)+b} \leqq C \,\| \boldsymbol{P}\phi \|_{\sigma+b}.$$

On the other hand, at ω:

$$\| [\boldsymbol{P}, U_p]\phi \|_{\sigma+b-2p+b} \leqq C \,\| \boldsymbol{P}\phi \|_{\sigma+b}.$$

We have therefore, at ω:

$$\| [\boldsymbol{P}\boldsymbol{U}_p, \boldsymbol{Q}]\phi \|_{\sigma+b-2p-\mu+b} \leqq C \,\| \boldsymbol{P}\phi \|_{\sigma+b}.$$

Then (7.1) gives the result.

Q. E. D.

Let us now take mollifiers ρ_t as in § 6. We shall consider the following property of a distribution u in Ω:

$(R)_\sigma$ *There is an open neighborhood* N_σ *of* ω *such that the following is true, for* $\phi \in C_0^\infty(N_\sigma)$:

i) $\boldsymbol{P}(\phi u) \in H^\sigma$;

ii) *when* $t \to 0$, $\boldsymbol{P}[\rho_{t*}(\phi u)] \to \boldsymbol{P}(\phi u)$ *weakly in* H^σ.

LEMMA 13. *Let* $\boldsymbol{P}$ *be regular of type* (s_0, a, b) *at* ω. *If* $u \in H^{s_0+m}{}_{\text{loc}}(\Omega)$ *and* $\boldsymbol{P}u \in H^s{}_{\text{loc}}(\Omega)$, *then* $(R)_s$ *holds.*

Since $u \in H^{s_0+m}{}_{\text{loc}}(\Omega)$, $(R_{s_0}$ is trivially true. Let us assume that $(R)_\sigma$ holds for some $\sigma \geqq s_0$. Of course we assume $s > \sigma$.

Let Ω''_σ be the open neighborhood of ω considered in Lemma 10 (where we take $\Omega' = \Omega$). Let us set

$$N'_\sigma = \Omega''_\sigma \cap N_\sigma.$$

Let U, V be two open neighborhoods of ω, with the following properties: $\bar{U}$, $\bar{V}$ are compact, $\bar{U} \subset V$, $\bar{V} \subset N'_\sigma$. If $\phi_1 \in C_0^\infty(V)$, we may find a number $t_0 > 0$ such that, for $t \leqq t_0$, $\rho_{t*}(\phi_1 u)$ has its support in N'_σ. Let $\phi \in C_0^\infty(U)$ and let us assume that $\phi_1 = 1$ on a neighborhood of $\bar{U}$. We have:

$$\boldsymbol{P}(\phi u) = \phi \boldsymbol{P}u + [\boldsymbol{P}, \phi](\phi_1 u).$$

We have then, for $t < t_0$,

$$\| [\boldsymbol{P}, \phi]\{\rho_{t*}(\phi_1 u)\} \|_{\sigma+b} \leqq C \, \| \boldsymbol{P}\{\rho_{t*}(\phi_1 u)\} \|_\sigma.$$

According to $(R)_\sigma$ the right hand side is uniformly bounded with respect to $t \to 0$. We use now the fact that closed bounded set are weakly compact in $H^{\sigma+b}$: the functions $[\boldsymbol{P}, \phi]\{\rho_{t*}(\phi_1 u)\}$ must weakly converge in $H^{\sigma+b}$ as $t \to 0$. Their limit can only be $[\boldsymbol{P}, \phi](\phi_1 u)$, which therefore belongs to $H^{\sigma+b}$.

Let c be a number $\geqq 0$, $c \leqq b$, $c \leqq s - \sigma$. Since $\sigma + c \leqq s$, $\phi \boldsymbol{P}u \in H^{\sigma+c}$; since $c \leqq b$, $[\boldsymbol{P}, \phi](\phi_1 u) \in H^{\sigma+c}$; hence $\boldsymbol{P}(\phi u) \in H^{\sigma+c}$.

This being done, we apply Lemma 11. There is an open neighborhood W of ω and a constant $C < +\infty$, both independent of $t \leqq t_0$ ($t_0 > 0$ sufficiently small), such that, for $\psi \in C_0^\infty$ with support in W,

$$\begin{aligned} \| \boldsymbol{P}(\rho_{t*}\psi) \|_{\sigma+c} &\leqq \| [\boldsymbol{P}, \rho_{t*}]\psi \|_{\sigma+c} + \| \rho_{t*}\boldsymbol{P}\psi \|_{\sigma+c} \\ &\leqq \| [\boldsymbol{P}, \rho_{t*}]\psi \|_{\sigma+b} + \| \rho_{t*}\boldsymbol{P}\psi \|_{\sigma+c} \\ &\leqq C \, \| \boldsymbol{P}\psi \|_\sigma + \| \rho_{t*}\boldsymbol{P}\psi \|_{\sigma+c}. \end{aligned}$$

Let U' be an open neighborhood of ω, such that U' is compact and $U' \subset W$. Let us set $\tilde{N}_{\sigma+c} = U \cap U'$. If $\phi \in C_0^\infty(\Omega)$ has its support in $\tilde{N}_{\sigma+c}$, $\psi = \rho_{\epsilon *}(\phi u)$ has its support in W as soon as $\epsilon > 0$ is small enough. On the other hand, $\boldsymbol{P}(\phi u) \in H^{\sigma+c}$.

When $\epsilon \to 0$,

i) $\rho_{t*}\boldsymbol{P}\psi \to \rho_{t*}\boldsymbol{P}(\phi u)$ in $H^{\sigma+c}$ trivially;

ii) $\boldsymbol{P}(\rho_{t*}\psi) \to \boldsymbol{P}(\rho_{t*}(\phi u))$ in $H^{\sigma+c}$ trivially;

iii) $\boldsymbol{P}\psi \to \boldsymbol{P}(\phi u)$ weakly in H^{σ} because of $(R)_\sigma$.

At the limit, we have:

$$\| \boldsymbol{P}(\rho_{t*}(\phi u)) \|_{\sigma+c} \leqq C \, \| \boldsymbol{P}(\phi u) \|_{\sigma} + \| \rho_{t*}\boldsymbol{P}(\phi u) \|_{\sigma+c}.$$

When $t \to 0$, $\rho_{t*}\boldsymbol{P}(\phi u) \to \boldsymbol{P}(\phi u)$ in $H^{\sigma+c}$ since $\boldsymbol{P}(\phi u) \in H^{\sigma+c}$. We derive from there that $\boldsymbol{P}(\rho_{t*}(\phi u))$ remains bounded in $H^{\sigma+c}$, therefore converges weakly in $H^{\sigma+c}$, necessarily to $\boldsymbol{P}(\phi u)$. We have thus proved that whatever be $s_0 \leqq \sigma \leqq s$, $(R)_\sigma \Longrightarrow (R)_{\sigma+c}$ for $c \geqq 0$, $c \leqq b$, $c \leqq s - \sigma$. Take an integer ν large enough so that $c = (s - s_0)/\nu \leqq b$. We have proved that for every $\mu = 0, \cdots, \nu - 1$, $(R)_{s_0+\mu c} \Longrightarrow (R)_{s_0+(\nu+1)c}$. For $\mu = \nu - 1$, we get $(R)_s$.

Lemma 14. *Same hypotheses as in Lemma* 13 *for* $\boldsymbol{P}$, u, $\boldsymbol{P}u$. *Then* ω *has an open neighborhood* U *such that* $\phi \in C_0^\infty(U)$ *implies* $\phi u \in H^{s+a}$.

Let us assume $s \geqq s_0$, for if s were $< s_0$, $s + a$ would be $< s_0 + m$ (since always $a \leqq m$) and since $u \in H^{s_0+m}{}_{\text{loc}}(\Omega)$, there would be nothing to prove.

We may first choose U in such a way that for t sufficiently small,

$$\| \rho_{t*}(\phi u) \|_{s+a} \leqq C \, \| \boldsymbol{P}(\rho_{t*}(\phi u)) \|_{s}.$$

If we take $U \subset N_s$ (neighborhood of ω, used in Property $(R)_s$), we see that the right hand side is uniformly bounded with respect to t. We derive from there that $\rho_{t*}(\phi u)$ converges weakly in H^{s+a} as $t \to 0$, necessarily to ϕu.

8. End of the proof of Theorem 1′. We make the assumption that $\boldsymbol{P}u \in H^{s}{}_{\text{loc}}(\Omega)$ (u: distribution on Ω). It is enough to prove the following: let ω be an arbitrary point of Ω and assume that $\boldsymbol{P}$ is of type $(s_0(\omega), a(\omega), b(\omega))$

at ω (according to Remark 5.1). Then there is an open neighborhood $U(\omega)$ of ω such that

$$\phi \in C_0^\infty(U(\omega)) \Longrightarrow \phi u \in H^{s+a(\omega)}.$$

For let then Ω_1 be an open subset of Ω, with compact closure. We may cover Ω_1 with a finite number of such open sets $U(\omega_1), \cdots, U(\omega_r)$ and take

$$a_1 = \inf(a(\omega_1), \cdots, a(\omega_r)).$$

In other words, we must extend the conclusion of Lemma 14 to an arbitrary distribution u in Ω. But if Ω_2 is open, $\bar{\Omega}_2$ compact, $\bar{\Omega}_1 \subset \Omega_2$, there is a real number q such that the restriction of u to Ω_2 belongs to $H_{\mathrm{loc}}{}^q(\Omega_2)$. We may therefore assume that $u \in H^q{}_{\mathrm{loc}}(\Omega)$.

Let ω be any point of Ω; let $x^1, \cdots, x^n$ be local coordinates near ω and let us introduce the operator

$$U_p = (1 - \frac{\Delta}{4\pi^2})^p, \ p\colon \text{integer} \geqq 0.$$

We assume that $\boldsymbol{P}$ is of order (s_0, a, b) at ω. Let us choose p large enough so that $q + 2p \geqq s_0{}^+ + m + b$, with $s_0{}^+ = \sup(s_0, 0)$. There is a distribution v on some neighbrohood Ω' of ω such that $u = U_p v$ in Ω'. And $v \in H^{q+2p}{}_{\mathrm{loc}}(\Omega') \subset H^{s_0{}^+ + m + b}{}_{\mathrm{loc}}(\Omega')$.

We have $\boldsymbol{P}U_p v \in H^s{}_{\mathrm{loc}}(\Omega')$. We know that $\boldsymbol{P}U_p$ is of type $(s_0{}^+ - 2p + b, a + 2p, b)$ (Lemma 12). Let us set $\tau_0 = s_0{}^+ - 2p + b$. We see that $v \in H^{\tau_0 + (m+2p)}{}_{\mathrm{loc}}(\Omega')$ and $m + 2p$ is precisely the order of $\boldsymbol{P}U_p$ near ω. We therefore apply Lemma 14, with $\boldsymbol{P}U_p$ instead of $\boldsymbol{P}$, Ω' instead of Ω, τ_0 instead of s_0, etc. There is an open neighborhood Ω^* of ω such that $\phi \in C_0{}^\infty(\Omega^*) \Longrightarrow \phi v \in H^{s+(a+2p)}$.

Let $\phi_1 \in C_0{}^\infty(\Omega^*)$ be identically one on some open neighborhood $\Omega^{**} \subset \Omega^*$ of ω; $\phi_1 v \in H^{s+(a+2p)}$. Let $\phi \in C_0{}^\infty(\Omega^{**})$. We have:

$$\phi u = \phi U_p v = \phi U_p(\phi_1 v).$$

But $U_p(\phi_1 v) \in H^{s+a}$.

9. Regularity of formally hypoelliptic operators. Let $P(D)$ be a differential operator with constant coefficients on R^n. Hörmander has proved (in [1]) that $P(D)$ is hypoelliptic if and only if there is a number $d > 0$

such that, for every multi-index $\alpha = (\alpha_1, \cdots, \alpha_r)$ $(1 \leqq \alpha_j \leqq n)$, $|\alpha| \geqq 1$, and for every $\xi \in R_n$,

$$(9.1) \qquad (1 + |\xi|^2)^{d/2} \, |P^{(\alpha)}(\xi)| \leqq C(1 + |P(\xi)|)$$

where $C < +\infty$ is independent of ξ.

Let Ω_1 be an open subset of a C^∞ manifold Ω covered by local coordinates $x^1, \cdots, x^n$. A differential operator $\boldsymbol{P}$ on Ω is said to be *formally hypoelliptic* in the local map $(\Omega_1, x^1, \cdots, x^n)$ if its expression $P(x, D)$ in the coordinates x^j satisfies the two following conditions:

$(FHE)_I$ *For every* $x_0 \in \Omega_1$, *the tangent differential operator* $P(x_0, D)$ (which has constant coefficients) *is hypoelliptic.*

$(FHE)_{II}$ *Whatever be the points* $x', x'' \in \Omega_1$, *there is a constant* $c > 0$ (depending on x', x'') *such that, for every* $\xi \in R_n$,

$$c \leqq \frac{1 + |P(x', \xi)|}{1 + |P(x'', \xi)|} \leqq \frac{1}{c}.$$

Several proofs of the hypoellipiticity of the formally hypoelliptic operators have been given (first by Hörmander [2] and Malgrange [1]; see also Peetre [1], Treves [1]). We shall indicate briefly the demonstration of the following fact:

THEOREM 2. *Let us assume that each point of* Ω *belongs to a local map in which* $\boldsymbol{P}$ *is formally hypoelliptic. Then* $\boldsymbol{P}$ *is regular in* Ω.

Since the question is of local nature, we may reason in a neighborhood of the origin in R^n (coordinates: $x^1, \cdots, x^n$). We may write

$$P(x, D) = P(0, D) + \sum_{j=1}^{N} a_j(x) P_j(D)$$

where, for every $j = 1, \cdots, N$, $a_j(x)$ is a C^∞ function in a neighborhood of 0, $a_j(0) = 0$, and $P_j(D)$ is hypoelliptic and satisfies

$$|P_j(\xi)| \leqq C(1 + |P(0, \xi)|), \qquad \xi \in R_n.$$

By hypothesis $P(0, D)$ is hypoelliptic. Now, whatever be s real, there is an open neighborhood O_s of 0 such that $\phi \in C_0^\infty(O_s)$ implies, whatever be the multi-index α of length $|\alpha| \geqq 1$,

$$\| P^{(\alpha)}(0,D)\phi \|_{s+d_0} \leqq C \| P(0,D)\phi \|_s; \tag{9.2}$$

$$\| P_j^{(\alpha)}(D)\phi \|_{s+d_j} \leqq C \| P_j(D)\phi \|_s \leqq C' \| P(0,D)\phi \|_s, \tag{9.3}$$

where $d_0 > 0$, $d_j > 0$. Furthermore if $s \geqq 0$, we will have, for those ϕ,

$$\| P(0,D)\phi \|_s \leqq C \| \boldsymbol{P}\phi \|_s. \tag{9.4}$$

For the proofs of these statements, see Malgrange [1].

There is a multi-index α such that $P^{(\alpha)}(0,\xi)$ is a constant $\neq 0$. If the order of $P(0,D)$ is $\geqq 1$ (which we may of course assume), $|\alpha| \geqq 1$ and by combining (9.2) and (9.4), we get, at the origin and for $s \geqq 0$,

$$\| \phi \|_{s+d_0} \leqq C \| \boldsymbol{P}\phi \|_s.$$

This proves (A_s) for $s \geqq 0$ and $a = d_0$.

In order to prove (B_s), it is enough to consider the case where $\boldsymbol{L}$ is of order $\mu = 0$, i.e. $\boldsymbol{L}$ is the multiplication by a C^∞ function ψ defined near ω, and the case where $\boldsymbol{L} = \dfrac{\partial}{\partial x^\lambda}$ for a certain λ, $1 \leqq \lambda \leqq n$.

We have

$$[\boldsymbol{P}, \psi] = \sum_{|\alpha|>0} \frac{D_\alpha \psi}{|\alpha|!} \{P^{(\alpha)}(0,D) + \sum_{j=1}^{N} a_j(x) P_j^{(\alpha)}(D)\}.$$

We may apply (9.2), (9.3). We get, at the origin

$$\| [\boldsymbol{P}, \psi]\phi \|_{s+d} \leqq C \| P(0,D)\phi \|_s$$

with $d = \inf(d_0, d_1, \cdots, d_N)$.

Then (9.4) yields, for $s \geqq 0$

$$\| [\boldsymbol{P}, \psi]\phi \|_{s+d} \leqq C \| \boldsymbol{P}\phi \|_s.$$

Last

$$[\boldsymbol{P}, \frac{\partial}{\partial x^\lambda}] = \sum_{j=1}^{N} \frac{\partial a_j}{\partial x^\lambda}(x) P_j(D).$$

We apply successively (9.3) and (9.4). For $s \geqq 0$,

$$\| [\boldsymbol{P}, \frac{\partial}{\partial x^{\lambda}}] \phi \|_{s+1} \leqq C \| \boldsymbol{P} \phi \|_{s+1}$$

is valid at the origin.

This proves (B_s) for $s \geqq 0$ and $b = \inf(d, 1)$ (actually, it is obvious that d is always $\leqq 1$; $d = 1$ if and only if $\boldsymbol{P}$ is elliptic).

REFERENCES.

[1] L. Hörmander, "On the theory of general partial differential operators," *Acta Mathematica*, vol. 94 (1955), p. 161.

[2] ———, "On interior regularity of solutions of partial differential equations," *Communications on Pure and Applied Mathematics*, vol. 11 (1958), p. 197.

[3] B. Malgrange, "Sur une classe d'opérateurs différentiels hypoelliptiques," *Bulletin de la Société Mathématique de France*, vol. 85 (1957), p. 283.

[4] J. Peetre, "Théorèmes de régularité pour quelques classes d'opérateurs différentiels," Thesis, Lund, 1959.

[5] F. Treves, "Opérateurs différentiels hypoelliptiques," *Ann. Inst. Fourier*, t. 9 (1959), p. 1.

PARTIALLY ANALYTIC SPACES.*

By Errett Bishop.

1. Introduction.

1. Introduction. The concept of a partially analytic space was introduced in a previous paper [1]. The present paper will refine and extend the theory. To this end it will be necessary to modify the definition of a partially analytic space which was given in [1]. Although formally quite different, the modified definition contains only one essentially new feature—local connectedness is no longer required.

Definition 1. *A partially analytic space* consists of a separable locally compact Hausdorff space K and a subalgebra $\mathfrak{A}$ of $C(K)$, where $C(K)$ is the algebra of all continuous complex-valued functions on K. The algebra $\mathfrak{A}$ contains the constant functions and is closed in the topology of uniform convergence on compact subsets of K. $\mathfrak{A}$ will be called the set of *analytic functions* on K.

In the previous paper certain structure manifolds were also postulated in the definition of a partially analytic space. The structure manifolds are now permitted to occur willy-nilly.

Definition 2. A *structure manifold* M of a partially analytic space K is a subset of K which has the structure of a complex analytic manifold such that (a) the manifold topology and the subset-of-K topology for M are the same, and (b) all functions in $\mathfrak{A}$ are analytic on M.

By *manifold* we mean connected separable complex analytic manifold.

Our first task is to show that the results of [1] remain valid for the more generally defined partially analytic spaces considered in this paper. This can be done by simple modifications of the proofs given in [1]. Proofs are only sketched. After this has been done we study a special kind of partially analytic space K, called an *embryonic space,* which is shown to have the property that the image of K under a proper analytic map of K into a manifold M is an analytic subset of M. This property of embryonic spaces is then applied to obtain simple proofs of two known results, (i) and (ii) below.

(i). Let A be an analytic set of dimension k in a manifold M. Let B be an analytic set in the manifold $M - A$ whose dimension at each point of

---

* Received May 11, 1961.

$M - A$ is at least $k+1$. We show that $\bar{B}$ is an embryonic space. Since the identity map of $\bar{B}$ into M is proper, we obtain as a corollary of the proper mapping theorem for embryonic spaces the Remmert-Stein theorem that $\bar{B}$ is an analytic subset of M. For this theorem see [9].

(ii). Let K be a holomorphically convex analytic space and $\mathfrak{A}$ a closed algebra of analytic functions on K with respect to which K is holomorphically convex. It is easy to see that the image K_0 of K under the natural map of K into $C^{\mathfrak{A}}$ (C denotes the complex numbers) is a separable locally compact Hausdorff space. The algebra $\mathfrak{A}$ can be considered as an algebra $\mathfrak{A}_0$ of functions on K_0, and together $\mathfrak{A}_0$ and K_0 constitute a partially analytic space. We show that this space is embryonic. From this fact we obtain Remmert's proper mapping theorem [8], which states that the image of an analytic space under a proper analytic map is an analytic subset of the image space.

If p is a point in a partially analytic space K, an n-tuple $f_1, \cdots, f_n$ of functions in $\mathfrak{A}$ will be said to be coordinates at the point p if there exists a neighborhood U of p which $f = (f_1, \cdots, f_n)$ maps properly into an open set $V \subset C^n$ such that for each h in $\mathfrak{A}$ there exists g analytic on V with $h/U = g \circ f$. Then K will be said to have rank at most n at p. We show that an embryonic space admits a set of coordinate functions at each point. It follows that an embryonic space can be canonically given the structure of an analytic space in the sense of Serre. Using this fact and the map described above of a holomorphically convex analytic space K onto a canonically associated embryonic space K we show that if $\mathfrak{A}$ is any closed algebra of analytic functions on K with respect to which K is holomorphically convex then there exists a canonical map ϕ of K onto an analytic space K_0 such that if $\mathfrak{A}_0$ denotes the set of functions f on K_0 such that $f \circ \phi \in \mathfrak{A}$ and if $\mathfrak{A}_{K_0}$ denotes the set of analytic functions on K_0 then $\mathfrak{A}_0 = \mathfrak{A}_{K_0}$. This theorem extends work of Stein [10], and has also been proved by Cartan [4], using other methods.

The theory of the imbedding of analytic spaces has been studied by Remmert, Narasimhan [7], and the author [1]. In this paper we study (Theorem 11) the problem of finding a proper analytic map of a holomorphically convex embryonic space K into complex Euclidean space C^N of sufficiently high dimension N which separates certain set of points of K and which locally generates all analytic functions at certain points of K. The imbedding theorems of [1] and [7] then follow as corollaries. The methods used for these constructions are basically those of [1] but also have something in common with the methods of [7].

The author is indebted to Hugo Rossi for many discussions about the

topics of this paper. Rossi has proved by different methods some results which are closely related to some of the results given below, in particular to Theorem 6 and to Corollary 2 of Theorem 8.

2. Partially analytic spaces.

Since a new definition has been given of partially analytic spaces it becomes necessary to redefine analytic polyhedra.

DEFINITION 3. A subset L of a partially analytic space K is called a *frame* if it is contained in the union of some countable family of structure manifolds of K. The *dimension* of L is the least integer d (possibly $d = \infty$) such that L is contained in the union of a countable set of structure manifolds on each of which $\mathfrak{A}$ has dimension at most d. Let $f_1, \cdots, f_n$ functions in $\mathfrak{A}$ and let L be a frame. Write

$$P_0 = \{p : p \in L, |f_i(p)| < 1, 1 \leqq i \leqq n\}.$$

Let P be a subset of P_0 which is both relatively open and relatively closed in P_0. If the closure P of P is a compact subset of L then P is called an *analytic polyhedron* with frame L defined by the functions $f_1, \cdots, f_n$. The *dimension* of P is the dimension of P when P itself is considered as a frame of K. P is called *reduced* if $n \leqq \dim P$, otherwise unreduced. An unreduced analytic polyhedron P is called *prepared* if it can be covered by a countable family $\{M_\alpha\}$ of structure manifolds such that for each α

(a) The dimension of $\mathfrak{A}$ on M_α does not exceed $\dim P$,

(b) For each α the algebra $\mathfrak{A}$ has dimension 0 on M_α over the set $(f_2f_1^{-1}, \cdots, f_nf_1^{-1})$.

Bdry P denotes the boundary of P when considered as a subset of its frame L.

The proof of the following theorem is the same as the proof of Theorem 3 of [1], except for one modification which will be discussed below.

THEOREM 1. *Let $\{L_j\}$ be a finite family of frames in the partially analytic space K. Let the functions $f_1, \cdots, f_n$ in $\mathfrak{A}$ define for each j an analytic polyhedron P_j with frame L_j. Let $\gamma = \gamma(j) \leqq n$ be the dimensions of P_j. Let S_j be a compact subset of P_j. Then there exist functions $f_1', \cdots, f_n'$ in $\mathfrak{A}$, which can be taken to be polynomial functions of the functions $f_1, \cdots, f_n$, such that for each j the functions $f_1', \cdots, f_\gamma'$ define an analytic polyhedron P_j' with frame L_j such that $S_j \subset P_j' \subset P_j$. If $|f_i| < 1$ for $1 \leqq i \leqq n$ at all points of a compact set $T \subset K$ then the functions f_i' may be taken to have the same property.*

Remarks on the Proof of Theorem 1. We need only consider the one place at which the proof of Theorem 3 of [1] needs to be modified. The modification is necessary because we have dropped the local-connectedness condition when defining the frame L of an analytic polyhedron P. Because of the absence of local connectedness for L, a union of components of P_0 need no longer be an analytic polyhedron. This means that the proof of Theorem 2 of [1] must be modified. Theorem 2 of [1] states, in part, that if a prepared analytic polyhedron P is defined by functions $f_1, \cdots, f_n$, if $S \subset P$ is compact, and if $r > 1$ has the property that

$$S \subset P \cap \{p \colon |f_i(p)| < r^{-1}, 1 \leqq i \leqq n\},$$

then for N supfficiently large the functions

$$(rf_i(p))^N - (rf_1(p))^N \qquad 2 \leqq i \leqq n$$

define an analytic polyhedron Q with $S \subset Q \subset P$. To see this write

$$Q_0 = \{p \colon p \in L, |(rf_i(p))^N - (rf_1(p))^N| < 1, \quad 2 \leqq i \leqq n\}.$$

In [1] it was sufficient to take Q to be the union of those components of Q_0 which intersect S, but this need not give an analytic polyhedron if L is not locally connected. Thus a different construction of Q is needed. Write $Q_1 = \bar{Q}_0 \cap P$. As in [1] it follows that if N is sufficiently large then S and $(\text{bdry} P) \cap Q_1$ are disjoint closed subsets of the compact Hausdorff space Q_1 which are simultaneously intersected by no component of Q_1. It follows (see [6], p. 158) that there exists an open and closed subset Q_2 of Q_1 which contains S and is disjoint from bdry P. Thus $Q = Q_2 \cap Q_0$ is an open and closed subset of $Q_0 \cap P$ which is disjoint from bdry of P. It follows that $S \subset Q \subset P$ and that Q is open and closed in Q_0. Thus Q is the desired analytic polyhedron. Thus Theorem 2 of [1] can be established even when L is not locally connected. The rest of the proof of Theorem 3 of [1] is the same. Theorem 3 of [1] is just Theorem 1 above, except for the remark that the f_i' can be taken to be polynomials in the f_i. To see this note that the theory holds if $\mathfrak{A}$ is replaced by the closed subalgebra of $\mathfrak{A}$ generated by the functions $f_1, \cdots, f_n$. This implies that the functions f_i' can be taken to be uniform limits on compact sets of polynomials in the functions f_i, from which it easily follows that they can be taken to be polynomials in the f_i. Finally, it is clear from the proof of Theorem 3 of [1] that the f_i' can be chosen to have absolute values less than 1 at all points of T.

The following definitions and theorem correspond to Definitions 6 and 7 and Theorem 4 of [1]. The proof is the same.

Definition 4. A partially analytic space K is called *weakly holomorphically convex* if K itself is a frame and if for each compact set $S \subset K$ each component of the set

$$S = \{p \in K : |f(p)| \leqq \max_{q \in S} |f(q)|, \text{ all } f \text{ in } \mathfrak{A}\}$$

is compact.

Definition 5. A continuous mapping ϕ of a topological space T_1 into a topological space T_2 is *almost proper* if each component of $\phi^{-1}(S)$ is compact for each compact set $S \subset T_2$.

Theorem 2. *Let* $\{L_j\}$ *be a finite family of closed frames of a weakly holomorphically convex partially analytic space* K, *with* $L_1 = K$. *Let the dimension* $\gamma = \gamma(j)$ *of* L_j *be finite for each* j. *Let* $n = \gamma(1)$ *be the dimension of* K. *Then the set of elements* $f = (f_1, \cdots, f_n)$ *of the* n*-fold Cartesian product* $\mathfrak{A}^n$ *of* $\mathfrak{A}$ *such that for each* j *the mapping*

$$f^j : p \to (f_1(p), \cdots, f_\gamma(p))$$

of L_j *into* C^γ *is almost proper is dense in* $\mathfrak{A}^n$.

3. Special frames. Definition 6 which follows replaces Definition 8 of [1].

Definition 6. A continuous proper map f from a subset S of a partially analytic space K to an n-dimensional complex analytic manifold M is called *special of dimension* n if all of the level sets of f on S are countable and if there exists a countable family $\{M_\alpha\}$ of n-dimensional structure manifolds of K which are subsets of S such that

(α) f is analytic on each M_α and non-singular on M_α at every point of M_α,

(β) Each M_α is open and $\cup M_\alpha$ is dense in S,

(γ) The set $H = f(S - \cup M_\alpha)$ is a countable union of locally analytic subsets of M, each of dimension at most $n - 1$.

It is worth noting that condition (α) may be replaced by the weaker condition

(α') f is analytic on each M_α and non-singular on M_α at *some* point of M_α.

To see this equivalence it is sufficient to note that if $\{M_\alpha\}$ satisfies (α'), (β), and (γ) and if A_α denotes the singular set of f on M_α then the family $\{M_\alpha'\}$, where $M_\alpha' = M_\alpha - A_\alpha$, satisfies (α), (β), and (γ). The only condition that is not obvious is (γ), and (γ) follows from the inclusion

$$f(S - \cup M_\alpha') \subset \cup f(A_\alpha) \cup f(S - \cup M_\alpha)$$

and the fact that $f(A_\alpha)$ is a countable union of locally analytic sets of dimensions at most $n - 1$.

Similarly we see that if the mapping f admits an extension to K such that $S - \cup M_\alpha$ is contained in the union of a countable family of structure manifolds of K of dimensions at most $n - 1$ on each of which f is analytic then f satisfies condition (γ).

Before stating the next theorem we recall from [1] that if X is a topological space then ${}_kX$ denotes the k-fold unordered product of X, consisting of all unordered k-tuples of elements of X with the natural topology.

THEOREM 3. *Let f be a special map from a subset S of a partially analytic space K into a complex analytic manifold M, and let $\{M_\alpha\}$ be a countable family of n-dimensional structure manifolds satisfiyng (α), (β), and (γ). Let $G = \cup M_\alpha$. Then $H = f(S - G)$ is closed and nowhere dense in M, and $M - H$ is connected. There exists an integer $\lambda \geqq 1$, called the multiplicity of the map f, such that for each point z in $M - H$ there exist exactly λ distinct points p in G with $f(p) = z$. The map ω from $M - H$ into ${}_\lambda S$ which takes z into the unordered λ-tuple of such points can be uniquely extended to a continuous map ω of M into ${}_\lambda S$.*

Proof. The proof is the same as the proof of Theorem 5 of [1], except where the proof of said theorem is incomplete. In the penultimate paragraph of the proof of Theorem 5 of [1] it is shown that ω can be continuously extended to $(E^n - H) \cup \{z_0\}$ for each z_0 in H. To do this it is assumed that there are only a finite number of points p in P with $f(p) = z_0$. This fact is not evident without further consideration. Assume therefore that the set Γ of points in P mapping into z_0 is infinite. Since Γ is a countable compact set in P, we see by the Baire category theorem that Γ has an infinite number of isolated points. Choose points $p_1, \cdots, p_{\lambda+1}$ which are isolated in Γ, and for $1 \leqq i \leqq \lambda + 1$ let U_i be a neighborhood of p_i with $\bar{U}_i \cap \Gamma = p_i$ such that the sets U_i are disjoint. As in the proof of Theorem 5 of [1] we see that there exists a neighborhood V of z_0 such that $f^{-1}(V) \cap \operatorname{bdry} U_i$ is void for all i. For each z in $V - H$ let $\delta_i(z)$, $1 \leqq i \leqq \lambda + 1$, be the number of points in $\omega(z) \cap U_i$. Since $V - H$ is connected we see that δ_i is constant on

$V - H$. Also $\delta_i \neq 0$ because if p is any point in $P - f^{-1}(H)$ sufficiently near to p_i then $f(p) = z \in U_i$ so that $\delta_i(z) \neq 0$. Thus

$$\lambda \geqq \sum \delta_i \geqq \lambda + 1,$$

a contradiction. Thus Γ is finite, as was to be proved.

COROLLARY. *If f is a special map from a subset S of a partially analytic space K into a complex analytic manifold M then the family $\{M_\alpha\}$ of Definition* 6 *can be taken to be a finite family of at most λ manifolds, such that $f(M_\alpha) \subset M - H$ for all α.*

Proof. Let A be the set of points p in M such that $\omega(p)$ consists of λ distinct points, so that A is open and dense in M. Because the complement of A has topological dimension at most $2n-2$, A is connected. Now $f^{-1}(A)$ is a λ-sheeted covering space of A. Since A is connected, the set $\{M_\alpha'\}$ of components of $f^{-1}(A)$ is finite. It is then clear that each M_α' has the structure of a complex analytic manifold and that $\{M_\alpha'\}$ satisfies conditions (α), (β), and (γ) of Definition 6.

Corresponding to Lemma 5 of [1] we have the following theorem and corollary

THEOREM 4. *Under the assumptions of Theorem* 3, *let h be a continuous function on M which is analytic on $M - H$. Then h is analytic on M.*

Proof. The proof is essentially contained in the proof of Lemma 5 of [1]. H. Rossi suggests the following simple proof of Theorem 4 by induction on the dimension n of M. If $n = 1$ then H is a countable closed subset of M, so that the set H_0 of points in M where f is not analytic is countable and closed. Thus H_0 is void since otherwise H_0 would contain isolated points, contradicting the fact that a continuous function does not have isolated points of non-analyticity. This proves the theorem for $n = 1$. Consider $n > 1$ and assume the theorem true for $n - 1$. We may assume that M is $E^n = \{(z_1, \cdot \cdot \cdot, z_n) : |z_i| < 1, 1 \leqq i \leqq n\}$. Thus the intersection of H with all but a countable set of the varieties

$$L_c = \{(z_1, \cdot \cdot \cdot, z_n) \in E^n : z_1 = c\}$$

is a countable union of locally analytic subsets of L_c, each of dimension at most $n - 2$. By the induction hypothesis, f is analytic on all such L_c. Thus f is analytic on M.

COROLLARY. *Under the assumptions of Theorem* 3, *let g be a continuous* *function on S which is analytic on each M_α and let s be a symmetric polynomial in variables $z_1, \cdots, z_\lambda$. For each z in M let $p_1, \cdots, p_\lambda$ denote the points of $\omega(z)$, counted according to multiplicity. Then the function h on M defined by*

$$h(z) = s(g(p_1), \cdots, g(p_\lambda))$$

is analytic on M.

Proof. By Theorem 4, it is sufficient to show that h is analytic at each point z_0 of $M - H$. Let $p_1{}^0, \cdots, p_\lambda{}^0$ be the points of $\omega(z_0)$. Thus z_0 has a neighborhood U such that there exist analytic homeomorphisms $\phi_1, \cdots, \phi_\lambda$ of z_0 onto neighborhoods of $p_1{}^0, \cdots, p_\lambda{}^0$ respectively with $\phi_i(z) \in \omega(z)$ for all z in U. Thus for all z in U we have

$$h(z) = s(g(\phi_1(z)), \cdots, g(\phi_\lambda(z))),$$

so that h is analytic at z_0, as was to be proved.

We now study conditions under which the image of a partially analytic space under proper maps will be an analytic subset of the image space.

LEMMA 1. *Let $f = (f_1, \cdots, f_n)$ be a special map of a subset S of a partially analytic space K into an n-dimensional manifold M. Let g be a continuous function on S with values in C^k which is analytic on each M_α, with $\{M_\alpha\}$ as in Definition 6. Let h be the map (f, g) of S into the manifold $\tilde{M} = M \times C^k$. Then $h(S)$ is an analytic subset of $\tilde{M}$.*

Proof. Consider a point r in $\tilde{M} - h(S)$, so that $r = (q, t_1, \cdots, t_k)$ where $q \in M$ and $t_1, \cdots, t_k$ are complex numbers. Let $q_1, \cdots, q_\lambda$ be the points in S which map into q under f, i.e., the points of $\omega(q)$ counted according to multiplicity. Thus for each i, $1 \leqq i \leqq \lambda$, there exists $j = j(i)$, $1 \leqq j \leqq k$, with $g_j(q_i) \neq t_j$. There thus exists a polynomial Δ_i in one variable such that $\Delta_i(t_j) = 1$ and $\Delta_i(g_j(q_i)) = 0$. Define the analytic function Δ on C^k by

$$\Delta(z_1, \cdots, z_k) = \prod_{i=1}^{\lambda} \Delta_i(z_{j(i)}).$$

Thus $\Delta(t_1, \cdots, t_k) = 1$ and $\Delta(g(q_i)) = 0$ for $1 \leqq i \leqq \lambda$. It follows that $\Delta = \Delta \circ g$ is a continuous function on S which is analytic on each M_α, with $\Delta(q_i) = 0$ for $1 \leqq i \leqq \lambda$. If for each p in M we let $p_1, \cdots, p_\lambda$ denote the points of $\omega(p)$ then by the corollary of Theorem 4 we seee that each of the elementary symmetric functions of the quantities $\Delta(p_1), \cdots, \Delta(p_\lambda)$ is an analytic function of the point p *in* M. Thus the function F on $\tilde{M}$ defined by

$$F(p, z_1, \cdots, z_k) = \prod_{i=1}^{\lambda} (\Delta(z_1, \cdots, z_k) - \Delta(p_i))$$

is analytic on M. Clearly

$$F(r) = F(q, t_1, \cdots, t_k) = \prod_{i=1}^{\lambda} (1 - \Delta(q_i)) = 1.$$

Also if $(p, z_1, \cdots, z_k)$ is in $h(S)$ then there exists i, $1 \leqq i \leqq \lambda$, such that $z_1 = g_1(p_i), \cdots, z_k = g_k(p_i)$. Hence $F(p, z_1, \cdots, z_k)$ has the factor $\Delta(z_1, \cdots, z_k) - \Delta(p_i) = \Delta(z_1, \cdots, z_k) - \Delta(g_1(p_i), \cdots, g_k(p_i)) = 0$. Thus F vanishes on $h(S)$ and $F(r) = 1$. Therefore $h(S)$ is an analytic set, as was to be proved.

DEFINITION 7. An n-dimensional frame L in a partially analytic space K is called *special* if there exists a countable family $\{M_\alpha\}$ of n-dimensional structure manifolds of K such that

(a) $M_\alpha \subset L$ for all α,

(b) Each M_α is an open set in L,

(c) The dimension of the frame $L - \cup M_\alpha$ is at most $n - 1$,

(d) $\cup M_\alpha$ is dense in L,

(e) There exists a set $N \supset L$ such that the level sets of $\mathfrak{A}$ on N are all countable and such that N is a countable union of structure manifolds of K.

The family $\{M_\alpha\}$ is called a *structural family* for the frame L.

It is clear that if L is a special frame of dimension n in a partially analytic space K then a proper map $f = (f_1, \cdots, f_n)$ with $f_i \in \mathfrak{A}$, $1 \leqq i \leqq n$, from L into an open subset of C^n whose level sets on L are all countable is special whenever L has a structural family $\{M_\alpha\}$ such that f is non-singular at some point of each M_α.

LEMMA 2. *Let $g = (g_1, \cdots, g_k)$, with $g_i \in \mathfrak{A}$, $1 \leqq i \leqq k$, be a proper map of an n-dimensional special frame L in a partially analytic space K into an open subset U of C^k. Then $g^{-1}(p_0) \cap L$ is finite for all p_0 in U.*

Proof. Consider a point p_0 in U. Since g is proper, there exists an analytic polyhedron Q with frame L defined by functions which are linear combinations of the functions $g_1, \cdots, g_k$ such that $g^{-1}(p_0) \subset Q$. Since the dimension of $\mathfrak{A}$ on L is n, there exist functions $f_1, \cdots, f_n$ in $\mathfrak{A}$ defining an analytic polyhedron P with $g^{-1}(p_0) \subset P$. By changing the functions $f_1, \cdots, f_n$ slightly we may assume, by Theorem 1 of [1], that $f_1, \cdots, f_n$ have countable level sets on N. Thus f is a special map of P into E^n. If we let h be the map (f, g) of P into $E^n \times U$, we see by Lemma 1 that $h(P)$ is an analytic subset of $E^n \times U$. Thus

$$T = h(P) \cap (E^n \times \{p_0\}) = f(g^{-1}(p_0)) \times \{p_0\}$$

is a compact analytic subset of $E^n \times U \subset C^{n+k}$. Therefore T is finite. Thus $f(g^{-1}(p_0))$ is finite. Since f is at most λ to one, $g^{-1}(p_0)$ is finite. This proves the lemma.

THEOREM 5. *If $g = (g_1, \cdots, g_k)$ is a proper map of an n-dimensional special frame L in a partially analytic space K into an open set $U \subset C^k$, where $g_i \in \mathfrak{A}$ for all i, then $g(L)$ is an analytic subset of U.*

Proof. Since g is proper, $g(L)$ is closed in U. Thus we need only check that $g(L)$ is analytic at each point p_0 in $g(L)$. Let $\mathfrak{A}_0$ be the closure in the topology of uniform convergence on compact subsets of K of the set of all polynomials in the functions $g_1, \cdots, g_k$, so that $(K, \mathfrak{A}_0)$ is a partially analytic space. Let V be a small neighborhood of p_0 with $\bar{V} \subset U$. Since the map g is proper there exists an analytic polyhedron Q in $(K, \mathfrak{A}_0)$ with frame L with $L \cap g^{-1}(\bar{V}) \subset Q$. By Theorem 1 there exists an analytic polyhedron P defined by functions $f_1, \cdots, f_n$ in $\mathfrak{A}_0$ with $L \cap g^{-1}(\bar{V}) \subset P \subset Q$. Thus f can be changed slightly such that each f_i is a polynomial function of $g_1, \cdots, g_k$. Thus f is a proper map from an analytic polyhedron $P \supset L \cap g^{-1}(V)$ into E^n, such that there exist polynomial functions $\Delta_1, \cdots, \Delta_n$ on C^k with

$$f_i(p) = \Delta_i(g_1(p), \cdots, g_k(p))$$

for all p in K. Since P is an open subset of the special frame L it is itself a special frame, so that by Lemma 2 f is a special map of P into E^n. By Lemma 1 we see that $(f, g)(P) = A$ is an analytic set in $E^n \times U$, which clearly consists of all $(\Delta(p), p)$ for $p \in g(P)$, where $\Delta = (\Delta_1, \cdots, \Delta_n)$. Let $\gamma_1, \cdots, \gamma_j$ be analytic functions defined on some neighborhood Ω in $E^n \times U$ of the point $(\Delta(p_0), p_0)$ whose set of common zeros is $A \cap \Omega$. Choose a neighborhood W of p_0 with $W \subset V$ such that $(\Delta(p), p) \in \Omega$ for all p in W. Let B be the set of zeros on W of the analytic functions $\gamma_1(\Delta(p), p), \cdots, \gamma_j(\Delta(p), p)$. If $p \in B$ then $(\Delta(p), p) \in A$ so that $p \in g(P) \subset g(L)$. If $p \in g(L) \cap W = g(P) \cap W$ then $(\Delta(p), p) \in A \cap \Omega$ so that $\gamma_1(\Delta(p), p) = \cdots = \gamma_j(\Delta(p), p) = 0$ and therefore $p \in B$. Thus $g(L) \cap W = B$ so $g(L)$ is analytic at the point p_0, as was to be proved.

DEFINITION 8. A frame L in a partially analytic space K which is the union of a countable family of closed special frames only finitely many of which intersect any compact subset of L is called an *embryonic frame.* If K itself is an embryonic frame then K is called an *embryonic space.*

For embryonic frames we have the following immediate corollary of Theorem 5.

COROLLARY. *If L is an embryonic frame and $f_1, \cdots, f_k$ in $\mathfrak{A}$ define a* *proper map of L into an open set U in C^k then $f(L)$ is an analytic subset of U.*

As a corollary of this corollary, we obtain the following theorem.

THEOREM OF REMMERT-STEIN. *Let A be a k-dimensional analytic subset of an open set $U \subset C^n$. Let B be an analytic set in $U - A$ of dimension at least $k+1$ at each of its points. Then $\bar{B} \cap U$ is an analytic subset of U.*

Proof. Let $K = A \cup B$ and let $\mathfrak{A}$ be the closure on K in the topology of uniform convergence on compact sets of all functions analytic in U. Thus $(K, \mathfrak{A})$ is a partially analytic space. Clearly $L = \bar{B} \cap U$ is an embryonic frame in K. Let f be the inclusion map of L in U. By the above corollary, $\bar{B} = f(L)$ is an analytic subset of U, as was to be proved.

4. Contractions of analytic spaces. The term *analytic space* will be used in the sense of Serre (see [5], p. 280).

DEFINITION 9. Let K be an analytic space and $\mathfrak{A}$ be a closed algebra of functions everywhere analytic on K. Assume that K is holomorphically convex in the sense that the set $\bar{S}$ of Definition 4 is compact for all compact $S \subset K$. Let K_0 be the image of K under the natural map ϕ of K into $C^{\mathfrak{A}}$. Since K is holomorphically convex, the map ϕ is proper and K_0 is closed in $C^{\mathfrak{A}}$, so that K_0 is locally compact. Let $\mathfrak{A}_0$ be the subalgebra of $C(K_0)$ consisting of all f in $C(K_0)$ such that $f \circ \phi \in \mathfrak{A}$. It is clear that $(K_0, \mathfrak{A}_0)$ is a holomorphically convex partially analytic space which we call the *contraction* of $(K, \mathfrak{A})$.

Of course Definition 9 could be made for an arbitrary partially analytic space K, but we shall only apply the construction to analytic spaces. The object of this section will be to show that $(K_0, \mathfrak{A}_0)$ is actually an embryonic space.

LEMMA 3. *With the notation of Definition 9, let M be a structure manifold of K on which $\mathfrak{A}$ has dimension n. Then $\phi(M)$ is a frame in K_0 of dimension at most n.*

Proof. The proof is by induction on the dimension d of M. If $d = 0$ the lemma is clearly true, so assume that the lemma is proved for all d smaller than the actual dimension d of M. Choose $f_1, \cdots, f_n$ in $\mathfrak{A}$ to have rank n at some point of M, and let A be the analytic subset of M at which these functions have rank less than n. Thus A is a countable union of structure manifolds of K each of dimension less than d on each of which $\mathfrak{A}$ has rank at most n. By the induction hypothesis $\phi(A)$ is a frame of dimension at most n. On the other hand, $M - A$ can be covered by a countable family

$\{M_\alpha\}$ manifolds each of which is mapped by $f_1,\cdots,f_n$ onto a connected open set L_α in C^n and on each of which $f_1,\cdots,f_n$ and $\mathfrak{A}$ have the same level sets. Thus L_α is naturally homeomorphic to $\phi(M_\alpha)$; the $\phi(M_\alpha)$ are thus a countable family of structure manifolds of K_0 on each of which $\mathfrak{A}_0$ has dimension n. Thus $\phi(M-A)$ is also a frame of dimension at most n. This completes the proof.

LEMMA 4. *Let S be an analytic space whose set R of regular points is connected and let $\mathfrak{A}$ be an algebra of analytic functions on S of dimension at most n at each point of R. Let M be any structure manifold of S. Then $\mathfrak{A}$ has dimension at most n on M.*

Proof. If d is the dimension of S then every level set of $\mathfrak{A}$ on R has dimension at least $d-n$ at each point. Therefore, by a known result ([3], Exp. XIV), every level set of $\mathfrak{A}$ on S has dimension at least $d-n$ at each point. Assume that the dimension of $\mathfrak{A}$ on M is larger than n. Thus there exists $f=(f_1,\cdots,f_{n+1})$ in $\mathfrak{A}^{n+1}$ having rank $n+1$ at some point of M, so that $f(M)$ contains an open set U of C^{n+1}. Now S can be covered by a countable family $\{M_\alpha\}$ of structure manifolds such that for each α either f has rank $n+1$ at every point of M_α or at no point of M_α. Let $\{M_\alpha'\}$ be the subfamily of $\{M_\alpha\}$ consisting of those M_α on which f has rank less than $n+1$. If p is any point in U then $f^{-1}(p)$ contains some level set of $\mathfrak{A}$ on S and therefore has dimension at least $d-n$. By the theorem on the dimension of a countable union of closed sets, $f^{-1}(p)\cap M_\alpha$ has dimension at least $d-n$ for some α. Since the dimension of M_α is at most d it follows that f does not have rank $n+1$ at all points of M_α, so that M_α is some M_α'. Thus U is covered by the sets $f(M_\alpha')$. Since f has rank less than $n+1$ at all points of M_α', $f(M_\alpha')$ is a countable union of closed sets of topological dimensions at most $2n$. Thus U is a countable union of closed sets of topological dimensions at most $2n$. This contradiction proves Lemma 4.

THEOREM 6. *With the notation of Definition 9, $(K_0,\mathfrak{A}_0)$ is an embryonic space.*

Proof. The analytic space K is the union of a countable family $\{M_\alpha\}$ of irreducible sets, only finitely many of which intersect any compact subset of K. Thus $\{\phi(M_\alpha)\}$ is a covering of K_0 by closed frames, only finitely many of which intersect any compact subset of K_0. Thus it is sufficient to show that each $\phi(M_\alpha)$ is an embryonic frame in K_0. It is therefore enough to show that $\phi(T)$ is an embryonic frame in K_0 for each irreducible analytic subset T of K. We will do this by an induction on the dimension d of T. The case $d=0$ is clear. Thus we assume that the statement has been verified for all T of dimension smaller than the dimension d of the given T. Let S be the set of singular points of T, so that $\dim S < d$. Since S is the union of of a countable family of irreducible analytic sets of dimensions less than d, only finitely many of which intersect any compact set, we see by the induction hypothesis that $\phi(S)$ is an embryonic frame in K_0. Thus if $\phi(S) = \phi(T)$ then $\phi(T)$ is an embryonic frame, as was to be proved. Therefore we may assume that $\phi(S) \neq \phi(T)$. We shall prove that the set $S_1 = T \cap \phi^{-1}(\phi(S))$ is an analytic subset of K. To this end, let p be any point in K, and let U be a neighborhood of p such that $\bar{U}$ is compact. Since K is holomorphically convex there exists an analytic polyhedron P with frame K_0 defined by functions $f_1, \cdots, f_n$ in $\mathfrak{A}_0$ such that $\phi(\bar{U}) \subset P$. Now let g be any element of $\mathfrak{A}^N$, where N is any positive integer and let $\hat{g}$ be the element of $\mathfrak{A}_0{}^N$ corresponding to g. Since $\phi(S)$ is an embryonic frame in K_0, $\phi(S) \cap P$ is an embryonic frame in the partially analytic space $(P, \mathfrak{A}')$ obtained by taking $\mathfrak{A}'$ to be all uniform limits on compact subsets of P of functions in $\mathfrak{A}_0$. By the corollary of Theorem 5 it follows that $(f_1, \cdots, f_n, \hat{g}) = \Delta$ maps $\phi(S) \cap P$ onto an analytic set B_g in $E^n \times C^N$. Hence the subset

$$U \cup (\Delta \circ \phi)^{-1}(B_g) = A_g = \{p \in U : (f_1(\phi(p)), \cdots, f_n(\phi(p)), g(p)) \in B_g\}$$

of U is analytic. Now clearly

$$U \cap \phi^{-1}(\phi(S)) = \bigcap A_g,$$

where the intersection is taken over all finite families g of functions in $\mathfrak{A}$. Thus $U \cap \phi^{-1}(\phi(S))$ is an analytic subset of U. It follows that $\phi^{-1}(\phi(S))$ is analytic subset of K. Thus $S_1 = T \cap \phi^{-1}(\phi(S))$ is an analytic set.

Now let k be the smallest of the local dimensions of all of the level sets of $\mathfrak{A}$ on T. By a known theorem ([3], Exp. XIV), the set J of p in T such that the level set of $\mathfrak{A}$ on T which passses through p has dimension k at p is an open set in T. Thus J intersects $T - S_1$ so that $\mathfrak{A}$ has rank $d - k$ at some point of $T - S_1$.

Now S_1 is the union of a countable family $\{M_\alpha\}$ of structure manifolds of K. Since the level sets of $\mathfrak{A}$ on S_1 have dimension at least k at each point, by Lemma 4 we see that $\mathfrak{A}$ is of dimension at most $d - 1 - k$ on each M_α. By Lemma 3 it follows that $\phi(S_1)$ is a frame in K_0 of dimension at most $d - k - 1$.

Now let S_2 be the set of all points in $T - S_2$ at which $\mathfrak{A}$ has rank $d - k - 1$ or less. Clearly S_2 is an analytic subset of $T - S_1$. Since $T - S_1$ is a (connected) manifold, S_2 is a proper analytic subset of $T - S_1$.

Now if $\mathfrak{A}$ had rank $d - k$ or more on S_2 at some regular point of S_2 then $\mathfrak{A}$ would have rank at least as great on $T - S_1$ at that point. Therefore

$\mathfrak{A}$ has rank at most $d-k-1$ at all regular points of S_2. Thus the dimensions of $\mathfrak{A}$ at every regular point of S_2 is at most $d-k-1$. By Lemma 4 it follows that S_2 can be covered by a countable family of structure manifolds on each of which $\mathfrak{A}$ has dimension at most $d-k-1$. Thus $\phi(S_2)$ is a frame in K_0 of dimension at most $d-k-1$. If $S_3 = S_2 \cup S_1$ it follows that the frame $\phi(S_3)$ in K_0 has dimension at most $d-k-1$. If $S_4 = T \cap \phi^{-1}(\phi(S_3))$ it follows that $H = T - S_4$ is open and dense in T and that $\phi(S_4) = \phi(S_3)$. Since $\mathfrak{A}$ has rank $d-k$ at each point of H, the level sets of $\mathfrak{A}$ on H will all be k-dimensional submanifolds of H or countable unions of such submanifolds. Now since the level sets of $\mathfrak{A}$ on H are closed in T, and therefore compact, each such level set will actually be a finite union of compact k-dimensional submanifolds M of H. Clearly the set $\tilde{H}$ of all such M has the structure of a $d-k$ dimensional manifold, and $\mathfrak{A}$ gives rise to an algebra $\tilde{\mathfrak{A}}$ of analytic functions on $\tilde{H}$ whose level sets on $\tilde{H}$ are all finite. Also $\tilde{\mathfrak{A}}$ has rank $d-k$ at each point of $\tilde{H}$ because $\mathfrak{A}$ has rank $d-k$ at each point of H.

Now if p_1 and p_2 are distinct points in $\tilde{H}$ with $h(p_1) = h(p_2)$ for all h in $\tilde{\mathfrak{A}}$, we may choose $(f_1, \cdots, f_{d-k}) = f$ in $\tilde{\mathfrak{A}}^{d-k}$ having rank $d-k$ at both p_1 and p_2, so that there exist neighborhoods U_1 and U_2 of p_1 and p_2 respectively each of which f maps homeomorphically onto the same open set $V \subset C^{d-k}$. Thus there exists a unique analytic homeomorphism σ of U_1 onto U_2 such that f and $f \circ \sigma$ agree on U_1. If $h \in \tilde{\mathfrak{A}}$ then the set

$$A_h = \{q \in U_1 \colon h(q) = h(\sigma(q))\}$$

is an analytic set in U_1. Clearly $\bigcap A_h = A$ is the set of all q in U_1 which are identified with some point in U_2 by all functions in $\tilde{\mathfrak{A}}$. If $A = U_1$ we write $p_1 \equiv p_2$. This clearly gives an equivalence relation on $\tilde{H}$, and the equivalence classes form a set $\hat{H}$ which has a canonical structure of a $d-k$ dimensional manifold in such a way that $\tilde{H}$ is a covering manifold of $\hat{H}$. Also $\tilde{\mathfrak{A}}$ gives rise to an algebra $\hat{\mathfrak{A}}$ of analytic functions on $\hat{H}$. If $p_1 \neq p_2$ in $\hat{H}$ and $h(p_1) = h(p_2)$ for all h in $\hat{\mathfrak{A}}$, define B_h just as A_h was defined, with $\tilde{H}$ replaced by $\hat{H}$ and $\tilde{\mathfrak{A}}$ by $\hat{\mathfrak{A}}$. Thus B is an analytic set in some neighborhood of p_1 and consists of all points in that neighborhood which are identified by $\hat{\mathfrak{A}}$ with some point in a fixed neighborhood of p_2. Since for each p_1 the number of possible p_2 is finite, it follows that there exists a neighborhood U of p_1 such that all points in U which are identified with some other point of $\hat{H}$ by all functions in $\hat{\mathfrak{A}}$ are a proper analytic subset of U. Thus the set W of all points in $\hat{H}$ which are identified with some other point in $\hat{H}$ by all functions in $\hat{\mathfrak{A}}$ is a proper analytic subset of $\hat{H}$.

If γ denotes the natural map of H onto $\hat{H}$ it follows that $\gamma^{-1}(W)$ is a proper analytic subset of H. As above we see that $\phi(\gamma^{-1}(W))$ is a frame in K_0 of dimension at most $d-k-1$. With $H_0 = H - \gamma^{-1}(W)$ it follows that $\phi(T-H_0) = \phi(\gamma^{-1}(W) \cup S_4)$ is a frame in K_0 of dimension at most $d-k-1$. Since H_0 is dense in T, $\phi(H_0)$ is dense in $\phi(T)$. Clearly $\phi(H_0)$ is in one-one correspondence with $\hat{H}-W$. It is easy to see that $\phi(H_0)$ and $\hat{H}-W$ are actually analytically homeomorphic in a natural way. Thus $\phi(H_0)$ is a $d-k$ dimensional structure manifold in K_0, at each point of which $\mathfrak{A}_0$ has rank $d-k$. Since $T-H_0$ is closed in T and therefore in K, $\phi(T-H_0)$ is closed in K_0. Since by construction $\phi(H_0)$ and $\phi(T-H_0)$ are disjoint, we see that $\phi(H_0)$ is open in the frame $\phi(T)$. It follows that $\phi(T)$ is a $d-k$ dimensional special frame in K_0, as was to be proved.

As a corollary, we obtain the proper mapping theorem of Remmert.

THEOREM. *If f is a proper analytic mapping of an analytic space K_1 into an analytic space K_2 then $f(K_1)$ is an analytic set in K_2.*

Proof. Since the analytic structure of K_2 is defined by local imbeddings of K_2 onto E^N for some N, there is no loss of generality in assuming that $K_2 = E^N$. Let K_0 be the contraction of $(K_1, \mathfrak{A})$, where $\mathfrak{A}$ is the algebra of all analytic functions on K_1. Since the coordinates of the mapping f are in $\mathfrak{A}$, we see that f gives rise to a proper analytic map $\bar{f}$ of K_0 into E^N, whose coordinates are in $\mathfrak{A}_0$. By Theorem 5 it follows that $f(K_1) = \bar{f}(K_0)$ is an analytic subset of E^N, as was to be proved.

5. Imbeddings and related maps.

DEFINITION 10. Let K be a partially analytic space. A set $S \subset \mathfrak{A}^N$ is *strictly of the first category* if it is contained in the union of a countable family $\{S_i\}$ of nowhere dense sets having the following property. For each i there exists a compact set $F_i \subset K$ and a closed subset J_i of $(C(F_i))^N$ such that S_i consists of all functions in $\mathfrak{A}^N$ whose restriction to F_i is in J_i.

THEOREM 7. *Let U and V each be a countable union of structure manifolds of dimensions at most n of a partially analytic space K. Let $f = (f_1, \cdots, f_n)$ in $\mathfrak{A}^n$ have countable level sets on $U \cup V$. For each p in U and q in V let there exist h in $\mathfrak{A}$ with $h(p) \neq h(q)$. Then the complement F of the set $G = G(U, V)$ of all g in $\mathfrak{A}^{n+1}$ for which $(f,g)(U)$ and $(f,g)(V)$ are disjoint is strictly of the first category in $\mathfrak{A}^{n+1}$.*

Proof. It is clearly enough to show that to each p in U and q in V there exist neighborhoods U' of p in U and V' of q in V such that the comcomplement of $G(U', V')$ is strictly of first category. This is clearly true unless $f(p) = f(q)$. Thus we may assume that U and V are mapped by f into the same open set Γ in C^n. Let $U = \cup U_k$, $V = \cup V_k$, where

$\{U_k\}$ and $\{V_k\}$ are countable families of compact sets. Let T_k consist of all g in $\mathfrak{A}^{n+1}$ such that $(f,g)(U_k)$ and $(f,g)(V_k)$ are disjoint. It is clearly sufficient to prove that for each k the complement S_k of T_k is strictly of first category. If we let J_k be the closure of S_k in $(C(U_k \cup V_k))^{n+1}$ it is sufficient to show that

(a) T_k is dense in $\mathfrak{A}^{n+1}$,

and

(b) For each g in T_k the restriction of g to $U_k \cup V_k$ is not in J_k.

We first prove (a). To this end, it is sufficient to show that the set T of all g in $\mathfrak{A}^{n+1}$ such that $(f,g)(U)$ and $(f,g)(V)$ are disjoint is dense. Consider therefore $g = (g_1, \cdots, g_{n+1})$ in $\mathfrak{A}^{n+1}$. Assume by induction on k that for each k, $0 \leqq k \leqq n+1$, there exist $g_1', \cdots, g_k'$ arbitrarily near to $g_1, \cdots, g_k$ respectively such that the set of points p in U with

$$(f(p), g_1'(p), \cdots, g_k'(p)) = (f(q), g_1'(q), \cdots, g_k'(q))$$

for some q in V is a frame L_k of dimension at most $n-k$, and the same for the corresponding frame M_k of V. This is clearly true if $k=0$. Thus by induction we may assume $g_1', \cdots, g_k'$ already chosen, $k < n+1$. The set of g_{k+1}' in $\mathfrak{A}$ such that for each frame L of a countable family of frames of dimensions at most $n-k$ covering L_k and each frame M of a countable family of frames of dimensions at most $n-k$ covering M_k there exists a dense countable set of points p in L and a dense countable set of points q in M such that

$$g_{k+1}'(p) \notin g_{k+1}'(V \cap f^{-1}(f(p)))$$

and

$$g_{k+1}'(q) \notin g_{k+1}'(U \cap f^{-1}(f(q)))$$

by obvious category arguments has a complement which is a set of first category in $\mathfrak{A}$. Thus we may find g_{k+1}' arbitrarily close to g_{k+1}. Now $(f, g_{k+1}')(M)$ is a countable union of locally analytic subsets of C^{n+k+1}, so that $A = L \cap (f, g_{k+1}')^{-1}(M)$ is a countable union of locally analytic subsets of L. Since by the choice of g_{k+1}' the set A has no interior in L, the frame A has dimension at most $n-k-1$. Since this is true for all L and M it follows that L_{k+1} and M_{k+1} are frames of dimensions at most $n-k-1$. This completes the induction. Letting $k=n+1$ we see that (a) is true.

To prove (b), notice that for each g in S_k the pair (f,g) identifies some point in U_k with some point in V_k. The same property therefore holds for J_k. From this (b) is clear and the lemma is proved.

COROLLARY. *If L is an n-dimensional frame, if $\mathfrak{A}$ separates points of L,* *and if* $f \in \mathfrak{A}^n$ *has countable level sets on* L *then the set* T *of all* g *in* $\mathfrak{A}^{n+1}$ *such that* (f,g) *is one-to-one on* L *has a complement* S *which is strictly of first category in* $\mathfrak{A}^{n+1}$.

Proof. The set $L \times L - \{(q,q) : q \in L\}$ can be covered by a countable family $\{U_k \times V_k\}$, where U_k and V_k are disjoint countable unions of frames of dimensions at most n. By the theorem, the complement of the set of all g such that $(f,g)(U_k)$ and $(f,g)(V_k)$ are disjoint is strictly of first category in $\mathfrak{A}^{n+1}$. From this the corollary follows easily.

DEFINITION 11. A point p in a frame L in a partially analytic space K is called an *analytic point* of L of dimension n and rank at most N if there exists a neighborhood U in L of p and f in $\mathfrak{A}^N$ mapping U homeomorphically onto an n-dimensional analytic subset of an open set $S \subset C^N$ such that for each h in $\mathfrak{A}$ there exists an analytic function w on S such that

$$h(p) = w(f(p))$$

for all p in U. Then f is called a set of coordinates at p and U is the corresponding coordinate neighborhood.

THEOREM 8. *Every point* p *of an embryonic frame* L *is an analytic point of* L *if* $\mathfrak{A}$ *separates points of* K.

Proof. By the corollary just proved, there exist $f_1, \cdots, f_N$ in $\mathfrak{A}$ mapping some neighborhood V of p one-to-one and properly onto an analytic set $A \subset E^N$. Let H consist of all continuous functions h on A such that there exists g in $\mathfrak{A}$ with $g(q) = h(f(q))$ for all q in U, and let G be the set of germs at $z = f(p)$ of H. Let F be the set of germs of all functions bounded and analytic in some neighborhood of z on the regular points of A, so F consists of the germs at z of all functions analytic on the normalization of A (see [5]). Let R consist of all functions in some neighborhood of z on A which can be extended to be analytic in some E^N neighborhood of z. Thus $R \subset G \subset F$, and G and F are R-modules. By the remark at the top of p. 291 of [5], the R-module F is finitely generated. Since R is noetherian, it follows that the sub-module G of F is also finitely generated. Thus there exist $g_1, \cdots, g_k$ in $\mathfrak{A}$ such that for each g in $\mathfrak{A}$ there exist $h_1, \cdots, h_k$ in R with

$$(*) \qquad \tilde{g}(t) = \sum_{i=1}^{k} h_i(t)\tilde{g}_i(t)$$

for all t in $A \cap V_g$, where V_g is some neighborhood of z and $\tilde{g}$ is the element in G corresponding to g in $\mathfrak{A}$. Thus if $\{S_n\}$ is a decreasing sequence of neighborhoods of z whose intersection is z, we see that for each g in $\mathfrak{A}$ there exists $n = n(g)$ with $S_n \subset V_g$ and $(h) \leqq n$, where

$$(h) = \sup\{|h_i(t)| : 1 \leqq i \leqq k, t \in S_n\}$$

with h_i as above. Hence $\mathfrak{A} = \cup \mu_n$, where

$$\mu_n = \{g : n(g) = n\}.$$

Since each μ_n is closed in $\mathfrak{A}$, some μ_n contains an open subset of $\mathfrak{A}$, for otherwise $\mathfrak{A}$ would be of first category. Thus actually $S_n \subset V_g$ for all g in $\mathfrak{A}$ for the right choice of V_g. Let $S = S_n \times C^k$, so that $f_0 = (f, g_1, \cdots, g_k)$ maps $f^{-1}(S_n) \cap U$ properly onto an analytic subset of S. For each g in $\mathfrak{A}$ we have (*), so that

$$g(q) = \sum_{i=1}^{k} h_i(f(q))\tilde{g}_i(f(q)) = \phi(f_0(q)),$$

for all q in $f^{-1}(S_n) \cap U$, where

$$\phi : (t, z_1, \cdots, z_k) \rightarrow \sum_{i=1}^{k} h_i(t) z_i$$

is analytic on S. This completes the proof.

COROLLARY 1. *Every embryonic space K for which $\mathfrak{A}$ separates points admits an analytic space structure K_0 so that all functions in $\mathfrak{A}$ are analytic on K_0. If K is holomorphically convex and if $\mathfrak{A}$ separates points of K then $\mathfrak{A}$ consists of all functions analytic on K_0.*

Proof. The first statement is an immediate consequence of Theorem 8. To prove the second statement, consider any h analytic on K_0. If S is any compact subset of K let P be an analytic polyhedron in K containing S defined by $f = (f_1, \cdots, f_n)$ in $\mathfrak{A}^n$. By Theorem 8, we may assume, by adding more functions if necessary, that $f_1, \cdots, f_n$ are a coordinate set of function at each point of P, and by the corollary to Theorem 7 we may assume that f separates points of P. Thus f maps P one-to-one onto an analytic set $A \subset E^n$. Let g be that function on A such that $h(p) = g(f(p))$ for all p in P. Since f is a coordinate system at each point of P and since h is analytic on K_0 the function g on A can be locally extended at each point of A to an analytic function in some neighborhood of that point. As is well known, it follows that g can be extended analytically to E^n. Thus g can be uniformly approximated on $f(S)$ by polynomials in the coordinate functions. It follows that h can be uniformly approximated on S by polynomials in the functions $f_1, \cdots, f_n$. Since S is any compact subset of K it follows that $h \in \mathfrak{A}$, as was to be proved. The author is indebted to Hugo Rossi for this argument.

COROLLARY 2. *Every holomorphically convex analytic space K admits an analytic proper map ϕ onto a holomorphically convex analytic space $\tilde{K}$ such that*

(a) *The algebra $\tilde{\mathfrak{A}}$ of analytic functions on $\tilde{K}$ separates point of $\tilde{K}$,*

(b) $\mathfrak{A} = \{f \circ \phi : f \in \tilde{\mathfrak{A}}\}$, *and*

(c) *There are enough analytic functions in* $\tilde{\mathfrak{A}}$ *to give a coordinate set of functions at each point of* $\tilde{K}$.

Proof. This corollary is an immediate consequence of Theorem 6 and Corollary 1 of Theorem 8.

THEOREM 9. *Let* p *be an analytic point of dimension* n *and rank at most* N *in a frame* L *of a partially analytic space* K, *so that there exists* $f = (f_1, \cdots, f_N)$ *in* $\mathfrak{A}^N$ *forming a coordinate set of functions on some neighborhood* U *of* p *and mapping* U *onto an analytic set* A *in an open set* M *of* C^N. *Let* $g = (g_1, \cdots, g_n)$ *be an element of* $\mathfrak{A}^n$ *all of whose level sets on* U *are countable. Then the set* T *of all* $h = (h_1, \cdots, h_N)$ *in* $\mathfrak{A}^N$ *such that* (g, h) *is a coordinate set of functions at all points of* U *has a complement* S *in* $\mathfrak{A}^N$ *which is strictly of first category.*

Proof. We may assume that $\bar{U}$ is a compact subset of L. Let $\{W_k\}$ be a sequence of compact subsets of U with $\cup W_k = U$. Let $\tilde{g}_1, \cdots, \tilde{g}_n$ be analytic functions on M with $g_i(p) = \tilde{g}_i(f(p))$ for all p in U and $1 \leqq i \leqq n$. For each k let T_k consist of all h in $\mathfrak{A}^N$ such that there exist analytic functions $\bar{h}_1, \cdots, \bar{h}_N$ on M for which $h_i(p) = \bar{h}_i(f(p))$ for all p in U and $1 \leqq i \leqq N$ with the property that $(\tilde{g}, \bar{h})$ has rank N at each point of $f(W_k)$. Clearly $T \supset \cap T_k$. Thus it is enough to show that for each k the complement S_k of T_k in $\mathfrak{A}^N$ is strictly of first category. If we let J_k be the closure of S_k in $(C(\bar{U}))^N$ it is sufficient to show that for each k

(a) T_k is dense in $\mathfrak{A}^N$

and

(b) For each h in T_k the restriction of h to $\bar{U}$ does not belong to J_k.

We first prove (a). To this end consider h in $\mathfrak{A}^N$. By induction on j, $0 \leqq j \leqq N$, we show that there exist functions $h_1', \cdots, h_j'$ in $\mathfrak{A}$ arbitrarily close to $h_1, \cdots, h_j$ respectively and $\bar{h}_1', \cdots, \bar{h}_j'$ as above such that for each r, $0 \leqq r \leqq N$, the set of points in A at which the rank of $(\tilde{g}, \bar{h}_1', \cdots, \bar{h}_j')$ on M is at most r has dimension at most $\max\{-1, r - j\}$. This is true for $j = 0$, for if $\tilde{g}$ had rank r or less on a set $B \subset A$ of dimension $r + 1$ then the level sets of g on the regular points of B would not be countable, contrary to the hypothesis on g. Thus we need only show how to find h_{j+1}', assuming that $j < N$ and $h_1', \cdots, h_j'$ have been found. For $0 \leqq r \leqq N$ let A_r be those points in A at which the rank of $(\tilde{g}, \bar{h}_1', \cdots, \bar{h}_j')$ on M is at most r. By the induction hypothesis either A_r is void or $\dim A_r \leqq r - j$. We consider $K \cup M$ as a topological space in which K and M are disjoint open sets with their given topologies. For $1 \leqq i \leqq N$ let the function $\hat{f}_i$ be defined on $K \cup M$ by $\hat{f}_i(p) = f_i(p)$ if $p \in K$ and $\hat{f}_i(z) = z_i$ if $z = (z_1, \cdots, z_N) \in M$.

Similarly define the function $\hat{h}_{j+1}$ on $K \cup M$ by $\hat{h}_{j+1}(p) = h_{j+1}(p)$ for p in K and $\hat{h}_{j+1}(z) = \bar{h}_{j+1}(z)$ for z in M, for a fixed choice of $\bar{h}_{j+1}$. Let $\hat{\mathfrak{A}}$ be the closed subalgebra of $C(K \cup M)$ generated by the functions $\hat{f}_1, \cdots, \hat{f}_N, \hat{h}_{j+1}$, so that $\hat{K}$ is a partially analytic space. If p is any regular point of $A_r - A_{r-1}$ it is easy to see that the set of all $\hat{h}_{j+1}'$ in $\hat{\mathfrak{A}}$ with the property that $(\tilde{g}, \bar{h}_1', \cdots, \bar{h}_j', \hat{h}_{j+1}')$ have rank $r + 1$ on M at p form an open dense set in $\hat{\mathfrak{A}}$. Thus there exists $\hat{h}_{j+1}'$ in $\hat{\mathfrak{A}}$ arbitrarily close to $\hat{h}_{j+1}$ such that for each r, $0 \leqq r \leqq N$, the functions $(\tilde{g}, \bar{h}_1', \cdots, \bar{h}_j', \hat{h}_{j+1}')$ have rank $r + 1$ at a dense set of regular points of $A_r - A_{r-1}$. Let h_{j+1}' be the restriction of $\hat{h}_{j+1}'$ to K and $\bar{h}_{j+1}'$ the restriction of $\hat{h}_{j+1}'$ to M. It follows that $(\tilde{g}, \bar{h}_1', \cdots, \bar{h}_{j+1}')$ can have rank r or less only on the union of A_{r-1} and a subset of A_r of dimension at most $\max\{-1, r - j - 1\}$; this union therefore has dimension at most $\max\{-1, r - j - 1\}$. Thus h_{j+1}' has the desired properties. By putting $j = N$ and $r = N - 1$ we see that $(\tilde{g}, \bar{h}_1', \cdots, \bar{h}_N')$ have rank N at each point of A, thus proving (a).

To prove (b), consider h in T_k. Thus $\bar{h}$ can be found so that $(\tilde{g}, \bar{h})$ has rank N of all points of $f(W_k)$. Now if h_0 in $\mathfrak{A}^N$ is close enough to h on the set $\bar{U}$ then by a theorem of Grauert and Remmert ([5], p. 291) $\bar{h}_0$ can be made arbitrarily close to $\bar{h}$ on some fixed neighborhood in M of $f(W_k)$. It follows that if h_0 is sufficiently close to h on $\bar{U}$ then $\bar{h}_0$ can be found such that $(\tilde{g}, \bar{h}_0)$ has rank N at all points of $f(W_k)$, so that h_0 is not in S_k. This clearly implies that h is not in J_k, thus proving (b).

The following lemma replaces Lemma 6 of [1]. The proof is the usual proof of this type of lemma.

LEMMA 5. *Let L be an embryonic frame, U an open subset of L, and S a compact subset of U such that for each p in $U - S$ there exists f in $\mathfrak{A}$ with*

$$|f(p)| > \sup\{|f(q)| : q \in S\}.$$

Let $\mathfrak{A}$ separate points of U. Let $1 \in \mathfrak{A}$. Let $\mathfrak{A}_0$ be the uniform closure of $\mathfrak{A}$ in $C(S)$. Then to every non-zero continuous homomorphism σ of $\mathfrak{A}_0$ into the complex numbers corresponds p_0 in S such that $\sigma(f) = f(p_0)$ for all f in $\mathfrak{A}_0$.

Proof. There exists an analytic polyhedron P with frame L, defined by functions $f = (f_1, \cdots, f_n)$ in $\mathfrak{A}$, such that $S \subset P \subset U$. By adding extra functions to f if necessary, we may assume by Theorems 7, 8, and 9 that f is a set of coordinates at each point of P and that f maps P one to-one onto an analytic set $A \subset E^n$. Thus each function in $\mathfrak{A}$ gives rise to an analytic function on A which can be extended to an analytic function on E^n. It follows that if S is identified with the set $f(S) \subset A$ then $\mathfrak{A}_0$ may be identified with the set of all uniform limits on $f(S)$ of functions analytic in E^n. Let z_0

be the point $z_0 = (\sigma(f_1), \cdots, \sigma(f_n))$ of E^n. To prove the lemma it will be sufficient to show that $z_0 \in f(S)$, for then p_0 can be taken to be that point of S with $f(p_0) = z_0$. To this end it is enough to show that for each z in $E^n - f(S)$ there exists h analytic on E^n with $|h(z)| > \sup\{|h(w)| : w \in f(S)\}$. This is clear if $z \in E^n - A$ for then there exists h which vanishes on A but not at z. If $z \in A - f(S)$ then by the hypothesis of the lemma there exists g in $\mathfrak{A}$ with $|g(p)| > \sup\{|g(q)| : q \in S\}$. If we let h be any function on E^n with $h \circ f = g$ on P, then h satisfies the requirement.

COROLLARY. *Under the hypotheses of Lemma 5 if S_1 and S_2 are disjoint closed sets with $S = S_1 \cup S_2$ then the function equal to 1 on S_1 and 0 on S_2 is in $\mathfrak{A}_0$.*

The next theorem extends Theorem 8 of [1]. The proof is the same.

THEOREM 10. *Let K be a holomorphically convex analytic space such that $1 \in \mathfrak{A}$ and $\mathfrak{A}$ separtes point of K. Let $f = (f_1, \cdots, f_n)$ be an almost proper map of K into C^n, $f_i \in \mathfrak{A}$. Let $\{S_k\}$ be a sequence of compact subsets of K such that $\cup S_k = K$ and $S_k \subset \operatorname{int} S_{k+1}$ for all k. Let*

$$J_k = \{z \in C^n : |z_i| \leqq k, 1 \leqq i \leqq n\}.$$

Let H_k be any compact subset of $f^{-1}(J_k)$ which is open in $f^{-1}(J_k)$ and contains $(S_k \cap f^{-1}(J_k)) \cup H_{k-1}$. Write

$$G_k = [f^{-1}(J_k) \cap H_{k+1}] - H_k$$

for $k \geqq 1$ and $G_0 = H_1$. For $k = 0, 1, \cdots$ let λ_k be any function in $\mathfrak{A}$ and ϵ_k any positive number. Let Γ be the set of all $g = (g_1, \cdots, g_N)$ in $\mathfrak{A}^N$ such that for all k, $k = 0, 1, \cdots$

$$|g_1(p) - \lambda_k(p)| < \epsilon_k, \quad p \text{ in } G_k.$$

Then Γ is not strictly of first category in $\mathfrak{A}^N$. If the sequence $\{\epsilon_k\}$ is bounded and if

$$\inf\{|\lambda_k(p)| : p \in G_k\} \to \infty \text{ as } k \to \infty$$

then (f, g_1) is a proper map of K into C^{n+1}.

Proof. Let $\{D_k\}$ be a sequence of compact subsets of K and F_k a closed subset of $(C(D_k))^N$ such that for each k the set $\bar{F}_k$ of all g in $\mathfrak{A}^N$ whose restriction to D_k is in F_k is nowhere dense in $\mathfrak{A}^N$. To show that Γ is not strictly of first category we must find g in $\Gamma - \cup \bar{F}_k$. By re-ordering and padding the sequence $\{D_k\}$ if necessary we may assume that $D_k \subset H_k$ for all k. We also assume that $\{\epsilon_k\}$ is a monotonely decreasing sequence. If $z = (z_1, \cdots, z_N)$ is an N-tuple of complex numbers define $|z| = \max\{|z_i|\}$. We construct by induction a sequence $g^0, g^1, \cdots$ of elements in $\mathfrak{A}^N$ such that

(a) $g^0+\cdots+g^k\notin \bar{F}_k$ for $k\geqq 1$,

(b) $|g^k(p)|<2^{-k-1}\min\{\epsilon_k,\delta_1,\cdots,\delta_{k-1}\}$ for $k\geqq 1$ and p in H_k, where δ_i is the distance in $(C(D_i))^N$ of $g^0+\cdots+g^i$ to F_i,

and

(c) $|g^0{}_1(p)+\cdots+g^k{}_1(p)-\lambda_k(p)|<\frac{1}{2}\epsilon_k$, $p\in G_k$ and $k=0,1,\cdots$.

To begin the induction take $g^0{}_1=\lambda_0, g^0{}_2,\cdots,g^0{}_N$ arbitrary. Assume that $g^0,\cdots,g^{k-1}$ have been constructed to satisfy the relevant conditions. Let U be a neighborhood of H_{k+1} such that $H_{k+1}=U\cap f^{-1}(J_{k+1})$. Thus for each p in $U-H_{k+1}$ for some i with $1\leqq i\leqq n$ we have

$$|f_i(p)|>k+1\geqq\sup\{|f_i(q)|:q\in H_{k+1}\}.$$

Since $G_k\cup H_k=f^{-1}(J_k)\cap H_{k+1}$ we see for p in

$$H_{k+1}-(G_k\cup H_k)\subset f^{-1}(J_{k+1})-f^{-1}(J_k)$$

that

$$|f_i(p)|\geqq k+1>k\geqq\sup\{|f_i(q)|:q\in G_k\cup H_k\}$$

for some i. It follows from Lemma 5 that there exists τ in $\mathfrak{A}$ arbitrarily near to 0 on H_k and to 1 on G_k. Write

$$g^k{}_1=-\tau(g^0{}_1+\cdots+g^{k-1}{}_1-\lambda_k)$$

and $g^k{}_i=0$, $2\leqq i\leqq N$. It is clear that if τ is chosen correctly then g^k satisfies (b) and (c). Thus by changing g^k slightly we may also assume that g^k satisfies (a).

Define $g=\sum_{k=0}^{\infty}g^k$. For each k this series converges uniformly on H_k because $|g^j(p)|<\epsilon_j2^{-j-1}$ for $p\in H_k$ whenever $j>k$. Thus $g\in\mathfrak{A}$, since for any compact $S\subset K$ there exists j with $S\subset S_j$, so that $S\subset H_k$ if k is chosen so large that $f(S_j)\subset J_k$. We see by (b) and (c) that for all p in G_k

$$|g_1(p)-\lambda_k(p)|\leqq|g^0{}_1(p)+\cdots+g^k{}_1(p)-\lambda_k(p)|$$
$$+\sum_{j=k+1}^{\infty}|g^j{}_1(p)|\leqq\tfrac{1}{2}\epsilon_k+\sum_{j=k+1}^{\infty}\epsilon_j2^{-j-1}<\epsilon_k.$$

Therefore $g\in\Gamma$. Also the distance in $(C(D_k))^N$ of g to F_k is at least

$$\delta_k-\sum_{j=k+1}^{\infty}\sup\{|g^j(p)|:p\in D_k\subset H_k\}\geqq\delta_k-\sum_{j=k+1}^{\infty}2^{-j-1}\delta_k>0.$$

This completes the proof that Γ is not strictly of first category. The rest of the theorem is proved as in [1].

We turn now to a consideration of certain imbedding properties. By Corollary 1 of Theorem 8 we see that every holomorphically convex embryonic space with a separating algebra $\mathfrak{A}$ of analytic functions can be realized as an analytic space which is holomorphically convex relative to the given algebra $\mathfrak{A}$, and by Theorem 6 in turn we see that the analytic space can be realized as a holomorphically convex embryonic space with a separating algebra $\mathfrak{A}$ of analytic functions. For this reason Theorem 10 holds for arbitrary holomirpically convex analytic or embryonic spaces, and the following theorem also yields information for such spaces.

THEOREM 11. *Let K be a holomorphically convex analytic space such that $1 \in \mathfrak{A}$ and $\mathfrak{A}$ separates points of K. Let K have dimension at most n at each point, so that by Theorem 2 there exists an almost proper map $f = (f_1, \cdots, f_n) \in \mathfrak{A}^n$ of K into C^n. Let $L_1, \cdots, L_k$ be a finite family of frames in K, and $U_1, \cdots, U_k$ open subsets of these respective frames, such that there exist integers $N_1, \cdots, N_k$ such that each point p of U_i, $1 \leqq i \leqq k$, is an analytic point of L_i of rank at most N_i. Write*

$$N = \max\{n+1, N_1, \cdots, N_k\}.$$

Then there exists $g = (g_1, \cdots, g_N)$ in $\mathfrak{A}^N$ such that

(a) *$(f, g_1, \cdots, g_{n+1})$ separates points of K,*

(b) *For each i, $1 \leqq i \leqq k$, the functions $(f, g_1, \cdots, g_{N_i})$ are coordinates at each point of U_i,*

(c) *(f, g_1) is a proper map of K into C^{n+1}.*

Proof. By Lemma 2 the level sets of f on K are all countable. By Theorem 7 the set T_1 of all g for which (a) is not true is strictly of first category in $\mathfrak{A}^N$. By Theorem 9 the set T_2 of all g for which (b) is not true is strictly of first category in $\mathfrak{A}^N$. Thus $T_1 \cup T_2$ is strictly of first category. By Theorem 10 there exists g in $K - (T_1 \cup T_2)$ which has property (c). This completes the proof.

Now we would like to improve Theorem 10 by choosing g so that the mapping $(f_1, \cdots, f_\gamma, g_1)$ is proper on certain embryonic frames L in K, where $\gamma = \dim L$ and $(f_1, \cdots, f_\gamma)$ is almost proper on L. Instead of showing that g can be so chosen we show in the next theorem that the map f can be chosen so that g_1 automatically satisfies the extra conditions. This theorem will at the same time be a considerable strengthening of Theorem 2.

THEOREM 12. *Let $\{L_j\}$ be a finite family of analytic sets of finite dimensions $\{\gamma = \gamma(j)\}$ in a d-dimensional holomorphically convex analytic space K. Then if $\mathfrak{A}$ is separating there exists $f = (f_1, \cdots, f_d)$ in $\mathfrak{A}^d$ such that*

(a) *For each j the mapping $f^j = (f_1, \cdots, f_\gamma)$ of L_j into C^γ is almost proper,*

(b) *For each j the functions $f_{\gamma+1}, \cdots, f_d$ vanish on L_j.*

Sketch of Proof. By decomposing each L_j into its homogeneous-dimensional parts we may assume that each L_j is a special frame. By lumping together all L_j of a given dimension we may assume that the L_j are special frames $L_1, L_2, \cdots, L_d$ of dimensions $1, 2, \cdots, d$ respectively. Finally, by enlarging the L_j appropriately we assume $L_1 \subset L_2 \subset \cdots \subset L_d = K$.

Now let S be any compact subset of K for which $S = \hat{S}$. We show by induction on k, $0 \leqq k \leqq d$, that there exist $h_1, \cdots, h_k$ in $\mathfrak{A}$ each of absolute value less than 1 on S such that for $1 \leqq j \leqq k$ the functions $h_{j+1}, \cdots, h_k$ vanish on L_j and such that $h_1, \cdots, h_j$ define an analytic polyhedron P_j in L_j with $S \cap L_j \subset P_j$. Since the case $k = 0$ is trivial, we may assume that $h_1, \cdots, h_{k-1}$ have been found with the desired properties. Consider p in $K - L_{k-1} - S$. Thus there exists w_1 in $\mathfrak{A}$ vanishing on L_{k-1} with $w_1(p) = 1$. Since $S = \hat{S}$ there exists w_2 in $\mathfrak{A}$ with $w_2(p) = 1$ and $|w_1(q) w_2(q)| < 1$ for all q in S. Thus there exist finitely many functions $g_1, \cdots, g_N$ in $\mathfrak{A}$ which vanish on L_{k-1} and have absolute values less than 1 on S such that $h_1, \cdots, h_{k-1}$, $g_1, \cdots, g_N$ define an analytic polyhedron Q in L_k with $S \cap L_k \subset Q$. By the construction used to prove Theorem 3 of [1], we may successively reduce the number N of such functions g, obtaining at the last step functions $h_1', \cdots, h_{k-1}'$, g_1' in $\mathfrak{A}$ having the desired properties for the functions $h_1, \cdots, h_k$ at the k-th stage. Thus we may assume that the functions $h_1, \cdots, h_d$ can be chosen for each compact set S with $S = \hat{S}$. Once this is done the proof of Theorem 4 of [1] can be repeated word for word to construct the desired functions $f_1, \cdots, f_d$.

University of California, Berkeley
and The Institute for Advanced Study.

REFERENCES.

[1] E. Bishop, "Mappings of partially analytic spaces," *American Journal of Mathematics*, vol. 83 (1961), pp. 209-242.

[2] H. Cartan, *Seminaire E. N. S.*, 1951-1952, Paris.

[3] ———, *Seminaire E. N. S.*, 1953-1954, Paris.

[4] ———, *Quotients of complex analytic spaces*, International Colloquium on Function Theory, Bombay, 1960.

[5] H. Grauert and R. Remmert, "Komplexe Räume," *Mathematische Annalen*, vol. 136 (1958), pp. 245-318.

[6] C. Kuratowski, *Topologie II*, Warsaw, 1950.

[7] R. Narasimhan, "Holomorphically complete complex spaces," *American Journal of Mathematics*, vol. 82 (1960), pp. 917-1934.

[8] R. Remmert, "Holomorphe und meromorphe Abildungen komplexer Räume," *Mathematische Annalen*, vol. 133 (1957), pp. 328-370.

[9] R. Remmert and K. Stein, "Über die wesentlichen Singularitäten analytischer Mengen," *Mathematische Annalen*, vol. 126 (1953), pp. 263-306.

[10] K. Stein, "Analytische Zerlegungen komplexer Räume," *Mathematische Annalen*, vol. 152 (1956), pp. 68-93.

ARITHMETICAL NOTES, V. A DIVISIBILITY PROPERTY OF THE DIVISOR FUNCTION.*

By ECKFORD COHEN.

---

1. **Introduction.** Let k and n denote positive integers, k fixed, and let $\tau(n)$ denote the number of (positive) divisors of n. The set of all n such that $k \mid \tau(n)$ will be denoted S_k and, for real $x \geqq 1$, the enumerative function (§ 2) of S_k will be denoted $S_k(x)$. Sathe [5] has investigated $S_k(x)$ for odd $k > 1$, obtaining the estimate,

$$S_k(x) \sim \alpha_k x \quad \text{as} \quad x \rightarrow \infty, \tag{1.1}$$

where α_k is a positive constant defined by (3.6). Sathe's proof depends upon a result [5, (3)] of S. Selberg and Pillai which is substantially equivalent to the Prime Number Theorem. It is the purpose of this note to prove a refinement of Sathe's estimate (Theorem 3.1). The method of the paper is elementary; in particular, no appeal is made to the theory of primes.

2. **Preliminaries.** The characteristic function $s(n)$ of a set S of positive integers n is defined by $s(n) = 1$ or 0 according as $n \in S$ or $n \notin S$. The enumerative function $S(x)$ of S is the summatory function of $s(n)$, that is, $S(x) = \sum_{n \leqq x} s(n)$. In this note Q will denote the set of square-free integers, and the characteristic and enumerative functions of Q will be denoted $q(n)$ and $Q(x)$, respectively. The symbol $a_k(n)$ will denote the characteristic function of the set A_k of the k-th powers. The Dedekind ψ-function is the arithmetical function,

$$\psi(n) = \sum_{d\delta = n} q(d)\delta, \qquad \psi(n)/n = \prod_{p \mid n} (1 + 1/p), \tag{2.1}$$

where the product is over the prime divisors of n. The number of square-free divisors of n will be denoted $\theta(n)$.

We recall a previously proved lemma.

LEMMA 2.1 ([2, Lemma 5.2]). *For positive integral r,*

$$Q_r^*(x) \equiv \sum_{\substack{n \leqq x \\ (n,r)=1}} q(n) = \beta(r)x + O(x^{\frac{1}{2}}\theta(r)) \tag{2.2}$$

where $\beta(r) = (6/\pi^2)r/\psi(r)$.

---

* Received May 24, 1961.

Remark 2.1. Clearly $\beta(n)$ is bounded.

Next we note a trivial though fundamental principle.

Remark 2.2. An integer n is *uniquely* representable as the product of a k-free integer by a k-th power.

Let $t_{k,r}(n)$ denote the characteristic function of the set $T_{k,r}$ of integers with a k-th power divisor whose complementary divisor is square-free and prime to r. Then by Remark 2.2

$$t_{k,r}(n) = \sum_{\substack{d\delta=n \\ (\delta,r)=1}} a_k(d)q(\delta). \tag{2.3}$$

We deduce now an estimate for the enumerative function $T_{k,r}(x)$ of the sequence $T_{k,r}$. Let $\zeta(s)$ denote the Riemann ζ-function, $s > 1$.

LEMMA 2.2. *For positive integral r and fixed $k \geqq 3$*

$$T_{k,r}(x) \equiv \sum_{n\leqq x} t_{k,r}(n) = \beta(r)\zeta(k)x + O(x^{1/k}\beta(r)) + O(x^{\frac{1}{2}}\theta(r)). \tag{2.4}$$

Proof. By (2.3) and Lemma 2.1,

$$\begin{aligned} T_{k,r}(x) &= \sum_{\substack{d\delta\leqq x \\ (\delta,r)=1}} a_k(d)q(\delta) = \sum_{n\leqq x} a_k(n)Q_r^*(x/n) \\ &= \beta(r)x\sum_{n\leqq x} a_k(n)n^{-1} + O(x^{\frac{1}{2}}\theta(r)\sum_{n\leqq x} a_k(n)n^{-\frac{1}{2}}) \\ &= \beta(r)x\sum_{n=1}^{\infty} n^{-k} + O(\beta(r)x\sum_{n>x^{1/k}} n^{-k}) + O(x^{\frac{1}{2}}\theta(r)\sum_{n\leqq x^{1/k}} n^{-k/2}), \end{aligned}$$

from which (2.4) results.

Let the integer n have the canonical factorization

$$n = p_1^{e_1}\cdots p_t^{e_t}, \qquad t = 0 \text{ if } n = 1, \tag{2.5}$$

where $p_1, \cdots, p_t$ denote the distinct prime factors of n. The set B of integers n in (2.5) with $e_i > 1$ for all i is the set of "square-full" integers. Let $B(x)$ represent the enumerative function of B and $b(n)$ its characteristic function.

LEMMA 2.3.

$$B(x) \equiv \sum_{n\leqq x} b(n) = O(x^{\frac{1}{2}}). \tag{2.6}$$

Proof. This estimate results from a much sharper approximation for $B(x)$ proved by Bateman in [1] using an elementary approach.

3. The main result. We introduce some further notation. The set of

k-free integers will be denoted Q_k, while the set of k-full integers namely, the integers n in (2.5) with $e_i \geqq k$ $(1 \leqq i \leqq t)$, will be represented by B_k. In particular, $Q = Q_2$ and $B = B_2$. If r is a positive integer $\leqq k$, then $F_{k,r}$ will be used to denote the intersection, $B_r \cap Q_k$, and $G_{k,r}$ the intersection, $F_{k,r} \cap S_k$. For simplicity, we write $F_k = F_{k,2}$, $G_k = G_{k,2}$, and use $g_k(n)$ and $G_k(x)$ to denote, respectively, the characteristic and enumerative functions of G_k.

Remark 3.1. It will be observed that $g_k(n) = 1$ if n is of the form (2.5) with $2 \leqq e_i \leqq k-1$ for all i and if $k \mid \tau(n)$, otherwise $g_k(n) = 0 (k \geqq 2)$. In particular, $G_k \subseteq F_k$.

The following representation for $s_k(n)$, the characteristic function of S_k, is basic for the main theorem.

LEMMA 3.1. *If k is odd and $\geqq 3$, then*

$$s_k(n) = \sum_{d\delta = n} g_k(d) t_{k,d}(\delta). \tag{3.1}$$

Proof. It may be seen (Remark 2.2) that an integer n has a *unique* factorization of the form,

$$n = d_1 d_2 d_3, \quad (d_1, d_3) = 1, \quad d_1 \in F_k, \quad d_2 \in A_k, \quad d_3 \in Q. \tag{3.2}$$

Moreover, if n is defined by (2.5), then $\tau(n) = (e_1 + 1) \cdots (e_t + 1)$, $\tau(1) = 1$. Hence, in the factorization (3.2), since k is odd and > 1,

$$n \in S_k \Longleftrightarrow d_1 \in G_k.$$

Thus, one obtains

$$s_k(n) = \sum_{\substack{d_1 d_2 d_3 = n \\ (d_1, d_3) = 1}} g_k(d_1) a_k(d_2) q(d_3),$$

which by (2.3) is the same as (3.1).

We mention two simple results that will be required. (Convention: vacuous products will be assumed to have the value 1).

LEMMA 3.2. *If $\epsilon < 1/r(r-1)$, then*

$$\sum_{\substack{n=1 \\ n \in F_{k,r}}} n^{\epsilon - 1/(r-1)} \qquad (k \geqq r \geqq 2) \tag{3.3}$$

is convergent.

Proof. We have

$$\sum_{\substack{n \leqq x \\ n \in F_{k,r}}} n^{\epsilon - 1/(r-1)} \leqq \prod_{i=r}^{k-1} \Big(\sum_{\substack{n \leqq x \\ n \in A_i}} n^{\epsilon - 1/(r-1)} \Big) \leqq \prod_{i=r}^{k-1} \zeta(i(1/(r-1) - \epsilon)).$$

Thus the convergence of (3.3) is assured.

LEMMA 3.3. *If* $x \geqq 2$, *then*

$$\sum_{n \leqq x} \tau(n)/n = O(\log^2 x). \tag{3.4}$$

For a much sharper (elementary) estimate of the sum on the left of (3.4), see [4, Lemma 71.3].

We are now in a position to prove our main result.

THEOREM 3.1. *If* k *is a fixed odd integer* $\geqq 3$, *then for* $x \geqq 2$

$$S_k(x) = \alpha_k x + O(x^{\frac{1}{2}} \log^2 x), \tag{3.5}$$

where

$$\alpha_k = \zeta(k) \sum_{n=1}^{\infty} g_k(n) \beta(n) n^{-1} = 6\pi^{-2} \zeta(k) \sum_{n=1}^{\infty} g_k(n)/\psi(n). \tag{3.6}$$

Proof. We first remark that the series in (3.6) is absolutely convergent, by the boundedness of $\beta(n)$ and the case $r = 2$ of Lemma 3.2 with $\epsilon = 0$.

By Lemma 3.1, it follows that

$$S_k(x) \equiv \sum_{n \leqq x} s_k(n) = \sum_{d\delta \leqq x} g_k(d) t_{k,d}(\delta) = \sum_{n \leqq x} g_k(n) T_{k,n}(x/n),$$

and hence, by Lemma 2.2 and Remark 2.1, that

$$\begin{aligned} S_k(x) = \zeta(k) x \sum_{n \leqq x} g_k(n) \beta(n) n^{-1} &+ O(x^{1/k} \sum_{n \leqq x} g_k(n) n^{-1/k}) \\ &+ O(x^{\frac{1}{2}} \sum_{n \leqq x} g_k(n) \theta(n) n^{-\frac{1}{2}}). \end{aligned} \tag{3.7}$$

Noting again that $\beta(n) = O(1)$, one obtains

$$\sum_{n \leqq x} g_k(n) \beta(n) n^{-1} = \sum_{n=1}^{\infty} g_k(n) \beta(n) n^{-1} + O(\sum_{n > x} g_k(n) n^{-1}).$$

Appealing to Lemma 3.2 $(r = 3)$, it follows (for some $C_k > 0$ depending on k alone) that

$$\begin{aligned} \sum_{n > x} g_k(n) n^{-1} \leqq \sum_{\substack{n^2 m > x \\ m \in F_{k,3}}} 1/n^2 m &= \sum_{\substack{m=1 \\ m \in F_{k,3}}}^{\infty} 1/m \sum_{n > (x/m)^{\frac{1}{2}}} 1/n^2 \\ &\leqq C_k x^{-\frac{1}{2}} \sum_{\substack{m=1 \\ m \in F_{k,3}}}^{\infty} m^{-\frac{1}{2}} = O(x^{-\frac{1}{2}}). \end{aligned}$$

Therefore

$$\sum_{n \leqq x} g_k(n) \beta(n) n^{-1} = \zeta^{-1}(k) \alpha_k + O(x^{-\frac{1}{2}}). \tag{3.8}$$

Noting that $G_k \subset B$, one obtains by partial summation and (3.6)

$$\sum_{n\leqq x} g_k(n)n^{-1/k} = \sum_{n\leqq x} G_k(n)\cdot n^{-1/k}(1-(1+1/n)^{-1/k}) + O(G_k(x)x^{-1/k})$$
$$= O(\sum_{n\leqq x} B(n)n^{-(1+1/k)}) + O(B(x)x^{-1/k})$$
$$= O(\sum_{n\leqq x} n^{-(1/k+\frac{1}{2})}) + O(x^{\frac{1}{2}-1/k}),$$

from which it results that

$$\sum_{n\leqq x} g_k(n)n^{-1/k} = O(x^{\frac{1}{2}-1/k}). \tag{3.9}$$

To complete the proof, we note the following simple properties of $\theta(n)$: $\theta(n)$ is multiplicative, $\theta(n^2)=\theta(n)$, and $\theta(n)=O(\tau(n))=O(n^\epsilon)$ for all $\epsilon>0$. Hence by Lemma 3.2 with $r=3$, $0<\epsilon<1/6$, one deduces that

$$\sum_{n\leqq x} g_k(n)\theta(n)n^{-\frac{1}{2}} \leqq \sum_{\substack{n^2m\leqq x\\(n,m)=1\\m\in F_{k,3}}} \theta(n^2m)\,(n^2m)^{-\frac{1}{2}} = \sum_{n\leqq x}\theta(n^2)/n \sum_{\substack{m\leqq x\\m\in F_{k,3}}} \theta(m)m^{-\frac{1}{2}}$$
$$= O(\sum_{n\leqq x}\theta(n)/n) = O(\sum_{n\leqq x}\tau(n)/n);$$

therefore by Lemma 3.3,

$$\sum_{n\leqq x} g_k(n)\theta(n)n^{-\frac{1}{2}} = O(\log^2 x). \tag{3.10}$$

The theorem follows on combining (3.7), (3.8), (3.9), and (3.10).

Remark 3.2. For the case in which k is a prime, a direct evaluation of α_k has been given by Sathe [5, Theorem 6]. For a much simpler, indirect evaluation of α_k in this case, the reader is referred to [3].

THE UNIVERSITY OF TENNESSEE.

REFERENCES.

[1] P. T. Bateman, "Solution to problem 4459," *American Mathematical Monthly*, vol. 61 (1954), pp. 477-479.

[2] Eckford Cohen, "Arithmetical functions associated with the unitary divisors of an integer," *Mathematische Zeitschrift*, vol. 74 (1960), pp. 66-80.

[3] ———, "Arithmetical Notes, IV. A set of integers related to the divisor function," *Journal of the Tennessee Academy of Science*, to appear.

[4] Trygve Nagell, "Introduction to Number Theory," *Uppsala*, 1951.

[5] L. G. Sathe, "On a congruence property of the divisor function," *American Journal of Mathematics*, vol. 67 (1945), pp. 397-406.

ON BOUNDARY VALUE PROBLEMS FOR LAPLACE'S EQUATION.*

By R. T. Seeley.[1]

Introduction. The object of this paper is to formulate certain boundary value problems for Laplace's equation in a way suitable for the representation of the boundary condition by a singular integral equation. This formulation is modeled to some extent on the Abel summation of Fourier series. The application considered is to show that, for a first order boundary operator that "covers" the Laplacian, the index of the problem is zero.

Section 1 describes the regions considered, and develops the results used to justify the representation of the boundary conditions by singular integral equations. Some lemmas used in this are proved in Section 3. Section 2 discusses the question of the index.

The methods used here may prove applicable to wide classes of elliptic boundary problems.

1. On the connection between u and $\partial u/\partial n$ for a harmonic function u.

Let $k \geqq 2$, and G be a bounded region in $k+1$ dimensional Euclidean space E^{k+1}, with boundary Γ. We assume that Γ is connected, and is almost a C_2 manifold, of dimension k. Specifically

i) Γ is a C_1 manifold; the unit normal at the point x in Γ is denoted by $\nu(x)$;

ii) there is a number $\tau > 0$ such that for every x in Γ the sphere of radius τ about $x \pm \tau\nu(x)$ intersects Γ only at x;

iii) for each t in $0 \leqq |t| \leqq \tau$, the points $\{x + t\nu(x);\ x \text{ in } \Gamma\}$ are all distinct and form a C_1 manifold Γ_t, bounding the region G_t; and

iv) if we introduce in E^{k+1} orthonormal coordinates $\xi_1, \cdots, \xi_k, \zeta$ with origin at the point x in Γ in such a way that the tangent plane to Γ at x is $\zeta = 0$, then in a neighborhood of x, Γ can be represented by $\zeta = h(\xi_1, \cdots, \xi_k)$, with h a C_1 function.

These conditions are not independent, of course.

It follows from these conditions that Γ_t is of the same type as Γ, with τ

---

* Received July 13, 1961.

[1] Currently at Mathematisch Centrum. Amsterdam.

replaced by $\tau - |t|$. Since the point x' on Γ_t nearest to the point x on Γ is $x' = x + t\nu(x)$, $\nu(x)$ is the normal to Γ_t at $x + t\nu(x)$.

It will be convenient to write simply ν instead of $\nu(x)$ in most contexts.

Let $d\sigma$ be the natural surface measure on Γ, and $|\Gamma| = \int_\Gamma d\sigma$. For a function f in $L^1(\Gamma)$, and x in E^{k+1}, let $Pf(x) = c\int_\Gamma f(y)\,|x - y|^{1-k} d\sigma_y$, where $c = \frac{1}{2}\Gamma((k-1)/2)\Pi^{-(k+1)/2}$, and $|x - y|^2 = \sum_1^{k+1} (x_i - y_i)^2$. $Pf(x)$ is harmonic when x is not on Γ; and since locally on Γ, P is dominated by convolution (in local coordinates) with a function in L^1, $Pf(x)$ is defined almost everywhere on Γ. For each t in $0 < |t| \leqq \tau$ and x in Γ we define $P_tf(x)$ by $P_tf(x) = Pf(x + t\nu)$. Lemma 1 proves that $P_tf \rightarrow P_0f$ in $L^1(\Gamma)$, and in $L^p(\Gamma)$ if f is in $L^p(\Gamma)$ $(1 \leqq p \leqq \infty)$; here P_0f is the restriction to Γ of Pf.

An operator N, the normal derivative, can be defined on the range of P_0 by $NP_0f(x) = \lim_{t \to 0-} D_tP_tf(x)$, where D_t denotes differentiation with respect to t. Lemma 2 shows that there is an operator K_0 (whose kernel is the adjoint of that for the double layer potential) such that $D_tP_tf \rightarrow f + K_0f$ in $L^p(\Gamma)$ as $t \rightarrow 0-$; the convergence is uniform if f is continuous. Thus $NP_0 = I + K_0$. The lemma shows moreover that if f is bounded, then K_0f is continuous; and that the kernel of K_0 is uniformly $0(|x - y|^{1-k})$.

The operator P_0 on $L^1(\Gamma)$ has trivial null space, as the following argument shows. Since $NP_0 = I + K$, the null space of P_0 is contained in that of $I + K_0$. This latter null space contains only continuous functions; for we can choose n so that the kernel of $K_0{}^n$ is bounded, so that if $f = -K_0f$, then $f = (-1)^n K_0{}^n f$ is bounded, from which it follows by Lemma 2 that $f = -K_0f$ is continuous. Thus if $P_0f = 0$ for f in $L^1(\Gamma)$, then f is continuous, and by Lemma 1 P_0f is the boundary value in the classical sense of the function Pf in E^{k+1}. It follows from the maximum principle that $Pf(x) = 0$ for all x in E^{k+1}. Now if $\phi(x)$ is any function in C_2 on E^{k+1}, with compact support, we have

$$\int_\Gamma \phi(x)f(x)\,d\sigma_x = c'\int_\Gamma\int_{E^{k+1}} |x - y|^{1-k}\Delta\phi(y)f(x)\,dy\,d\sigma_x$$
$$= c''\int_{E^{k+1}} \Delta\phi(y)Pf(y)\,dy = 0.$$

It follows that $f(x) \equiv 0$ on Γ.

We can also show that $NP_0f = 0$ only if P_0f is constant. For we have seen that if $NP_0 f = 0$, then f is continuous; thus Lemmas 1 and 2 yield for $u(x) = Pf(x)$ that

$$0 = \int_\Gamma u\,\partial u/\partial n = \lim_{t\to 0-} \int_{\Gamma_t} u\,\partial u/\partial n = \lim_{t\to 0-} \int_{G_t} |\nabla u|^2 = \int_G |\nabla u|^2.$$

This shows that $u = Pf$ is constant inside G, so that $P_0 f$ is constant.

For f in $L^p(\Gamma)$ and g in $L^q(\Gamma)$ we have $(NP_0 f, P_0 g) = (P_0 f, NP_0 g)$; this can be verified by approximating f and g with continuous functions and applying the formula

$$\int_\Gamma \overline{(P_0 g)}\,\partial Pf/\partial n = \int_G \overline{(\nabla Pg)} \cdot (\nabla Pf) = \int_\Gamma P_0 f\,\overline{(\partial Pg/\partial n)},$$

or by using the same formula on Γ_t and letting $t \to 0-$. Part of the same argument, with $f = g$, shows that $(NP_0 f, P_0 f) \geqq 0$.

If A is the averaging operator, i.e. $Af(x) = |\Gamma|^{-1} \int_\Gamma f(y)\,d\sigma_y$, then $ANP_0 = 0$; for by Lemma 2

$$\int_\Gamma NP_0 f = \lim_{t\to 0-} \int_{\Gamma_t} D_t Pf(x + t\nu)\,d\sigma_{x'} \qquad (x' = x + t\nu),$$

and the latter integral is $\int_{\Gamma_t} \partial u/\partial n$ for a function u harmonic in Γ_t and its interior. Now $(A + N)P_0$ has trivial null space. For if f is in $L^1(\Gamma)$ and $(A + N)P_0 f = 0$, then $0 = (A^2 + AN)P_0 f = AP_0 f$, which gives also $NP_0 f = 0$. This last equality implies $P_0 f$ is constant, and $0 = AP_0 f$ shows that this constant is zero. Thus $(A + N)P_0 = I + K_0 + AP_0 = I + L$, where the kernel $L(x, y)$ of L differs from the kernel of K_0 by a continuous function of y; and $I + L$ has trivial null space.

Now we can construct a right inverse J_0 for $A + N$, using P_0 as parametrix. Set $J_0 = P_0 + P_0 F$, where F is an integral operator to be determined. $(A + N)J_0 = I + L + F + LF$, so we seek F as a solution of $(I + L)F = -L$. F can be determined as an integral operator with kernel $F(x, y)$ given by $F(x, y) + \int_\Gamma L(x, z)F(z, y)\,d\sigma_z = -L(x, y)$. Since $I + L$ has trivial null space when acting on $L^1(\Gamma)$, this equation has, for each y in Γ, a unique solution $F(x, y)$ in $L^1(\Gamma)$. The kernel $F(x, y)$ constructed in this way has a singularity like that of $L(x, y)$, and so defines an operator F on $L^1(\Gamma)$ such that $F + LF = -L$, as desired.

From what we have shown about P_0, any function $P_0 f$ in its range is the boundary value of the harmonic function $u = Pf$ in G, with $\partial u/\partial n = NP_0 f$ on Γ, both boundary values being assumed in the L^p sense if f is in $L^p(\Gamma)$.

Thus any function $J_0 f$ in the range of $J_0 = P_0(I+F)$ is the boundary value of a harmonic function $u = P(I+F)f$, and on Γ $\partial u/\partial n = NP_0(I+F)f = NJ_0 f = f - AJ_0 f$. Since $ANP_0 = 0$, we find $Af - A^2 J_0 f$ or, since $A^2 = A$,

1) $$AJ_0 f = Af.$$

Thus $\partial u/\partial n = f - Af$. The function

$$J(\boldsymbol{x},\boldsymbol{y}) = c\,|\,\boldsymbol{x} - \boldsymbol{y}\,|^{1-k} + c\int_\Gamma |\,\boldsymbol{x} - \boldsymbol{z}\,|^{1-k} F(\boldsymbol{z},\boldsymbol{y})\, d\sigma_{\boldsymbol{z}}$$

with $\boldsymbol{x}$ in E^{k+1} and $\boldsymbol{y}$ in Γ, is then the Neumann function for G.

The results we have just obtained can be formulated as follows.

THEOREM 1. *If f is in $L^p(\Gamma)$, $1 \leqq p < \infty$, then there is a function $u(\boldsymbol{x})$ harmonic in G, given by $u = P(I+F)f$, such that*

$$\int_\Gamma |\, D_t u(\boldsymbol{x} + t\boldsymbol{\nu}) - f(\boldsymbol{x}) + Af\,|^p\, d\sigma \to 0,$$

and

$$\int_\Gamma |\, u(\boldsymbol{x} + t\boldsymbol{\nu}) - J_0 f(\boldsymbol{x})\,|^p d\sigma \to 0,$$

as $t \to 0-$. If f is bounded, $u(\boldsymbol{x} + t\boldsymbol{\nu}) \to J_0 f(\boldsymbol{x})$ uniformly. If f is continuous, $D_t u(\boldsymbol{x} + t\boldsymbol{\nu}) \to f(\boldsymbol{x}) - Af$ uniformly.

In order to state our next result, the uniqueness result corresponding to Theorem 1, in the best way, we need the formula

1a) $$J_0 A f = Af,$$

or what amounts to the same thing, that $J_0\phi = \phi$ if ϕ is constant. Suppose ϕ constant, and let $u = P(I+F)\phi$; then by Theorem 1 $\partial u/\partial n = \phi - A\phi = 0$. This boundary value is assumed uniformly, so by classical potential theory u is constant. Hence on Γ, $u = J_0\phi$ is constant. To evaluate the constant, we take averages and use (1) to obtain $J_0\phi = AJ_0\phi = A\phi = \phi$, which establishes 1a).

We can now establish the following converse of Theorem 1.

THEOREM 2. *If u is harmonic in G, and f is a function in $L^p(\Gamma)$, $(1 \leqq p < \infty)$, such that $\int_\Gamma |\, D_t u(\boldsymbol{x} + t\boldsymbol{\nu}) - f(\boldsymbol{x})\,|^p d\sigma \to 0$ as $t \to 0-$, then there is a function g in $L^p(\Gamma)$ such that $\int_\Gamma |\, u(\boldsymbol{x} + t\boldsymbol{\nu}) - g(\boldsymbol{x})\,|^p d\sigma \to 0$ as $t \to 0-$, and $g = J_0(f + Ag)$.*

The theorem is easy to establish if we assume that $\partial u/\partial n$ and u assume uniformly their respective boundary values f and g. For if $D_t u(x+t\nu)\to f(x)$ uniformly as $t\to 0-$, and for some g $u(x+t\nu)\to g(x)$ uniformly as $t\to 0-$, then the function $v(x)=u(x)-P(I+F)f(x)$ satisfies $\partial v/\partial n=0$ on Γ, in the classical sense, so v is constant. Since f is $\partial u/\partial n$, we have $\int_\Gamma f=0$, by (1), $\int_\Gamma P(I+F)f=\int_\Gamma J_0 f=\int_\Gamma f=0$. Then we can evaluate the constant value of v by averaging it on Γ, which leads to $v=Ag$, $u=P(I+F)f+Ag$, and $g=J_0 f+Ag=J_0(f+Ag)$.

We can obtain the general result by applying this special case to the manifolds Γ_t for $t<0$. To this end, let x' and y' be on Γ_t, $-\tau\leqq t<0$, and let L_t, F_t, and J_t be the operators on $L^1(\Gamma_t)$ with kernels

$$\begin{aligned} L_t(x',y') &= c\,|\Gamma_t|^{-1}\int_{\Gamma_t}|x'-y'|^{1-k}d\sigma_{x'} \\ &\qquad\qquad + (1-k)c(x'-y')\cdot\nu(x')\,|x'-y'|^{-1-k} \\ F_t(x',y') &= -L_t(x',y') - \int_{\Gamma_t}L_t(x',z')F_t(z',y')\,d\sigma_{z'} \\ J_t(x',y') &= c\,|x'-y'|^{1-k}+c\int_{\Gamma_t}|x'-z'|^{1-k}F_t(z',y')\,d\sigma_{z'}; \end{aligned} \tag{2}$$

these are for Γ_t what L, F, and J_0 are for Γ. Then if $\Delta u=0$ in G, it follows that u and $\partial u/\partial n$ assume their boundary values on Γ_t uniformly, so that by our preliminary result we have on Γ_t

$$u(x')-|\Gamma_t|^{-1}\int_{\Gamma_t}u(x')\,d\sigma_{x'}=\int_{\Gamma_t}J_t(x',y')\,(\partial u/\partial n)\,(y')\,d\sigma_{y'}. \tag{3}$$

Now let $v_t(x)$ be such that $\int_{\Gamma_t}\phi(x')\,d\sigma_{x'}=\int_\Gamma \phi(x+t\nu)v_t(x)\,d\sigma_x$ for every continuous function ϕ. Then $v_t(x)\to 1$ uniformly in x as $t\to 0$. Since $\nu(x)$ is the normal to Γ_t at $x+t\nu(x)$, $\partial u/\partial n$ on Γ_t is $D_t u(x+t\nu(x))$; thus relation (3) on Γ_t can be written

$$\begin{aligned} u(x+t\nu(x))-|\Gamma_t|^{-1}&\int_\Gamma u(x+t\nu))v_t(x)\,d\sigma \\ &=\int_\Gamma J_t(x+t\nu(x),y+t\nu(y))D_t u(y+t\nu(y))v_t(y)\,d\sigma_y. \end{aligned} \tag{4}$$

In order to obtain a limiting relation as $t\to 0-$, define the operator J^t on $L^1(\Gamma)$ by the kernel

$$J^t(x,y)=J_t(x+t\nu(x),y+t\nu(y))v_t(y); \tag{5}$$

Define A^t on $L^1(\Gamma)$ by $A^t f = |\Gamma_t|^{-1} \int_\Gamma f v_t d\sigma$; and define u_t on Γ by $u_t(x) = u(x + t\nu(x))$. Then according to (4),

$$u_t - A^t u_t = J^t D_t u_t \text{ for } -\tau \leqq t < 0. \tag{6}$$

Now by Lemma 3, $\| J^t - J_0 \| \to 0$ as $t \to 0-$, and the hypothesis of Theorem 2 is that $\| D_t u_t - f \| \to 0$, where $\| \cdot \|$ denotes the norm of an operator on, or a function in, $L^p(\Gamma)$. It follows that $J^t D_t u_t \to J_0 f$ in $L^1(\Gamma)$, and that $u_t - A^t u_t$ does the same.

Thus it remains only to show that there is a function g in $L^p(\Gamma)$ such that $u_t \to g$; it will then follow that $A^t u_t \to Ag$, and $g - Ag = J_0 f$, or $g = J_0(f + Ag)$, as desired. To find g, consider first $I(t) = \int_\Gamma u_t$. Then $I'(t) = \int_\Gamma D_t u_t \to \int_\Gamma f$, so that $I'(t)$ is bounded on $-\tau \leqq t < 0$ and $\lim\limits_{t\to 0-} I(t)$ exists. Now from (6), $\lim\limits_{t\to 0-} |\Gamma|^{-1} \int_\Gamma (u_t - A^t u_t) = |\Gamma|^{-1} \int_\Gamma J_0 f$; we have just seen that $\lim \int_\Gamma u_t$ exists, so it follows that $\lim A^t u_t$ exists. Finally, we obtain that $u_t = A^t u_t + J^t D_t u_t$ converges in $L^1(\Gamma)$ to $g = \lim\limits_{t\to 0-} A^t u_t + J_0 f$. This concludes the proof of Theorem 2.

2. More general boundary value problems. Theorems 1 and 2 are existence and uniqueness theorems respectively for the L^p formulation of the Neumann problem. In this section we consider more general first order boundary conditions, but require that $\partial u/\partial n$ exist on Γ in the L^p sense, for some $p > 1$. This is reasonable if the boundary operator is actually of first order at all points of Γ.

Specifically, we look for a function u such that

i) $\Delta u = 0$ in G,

β) ii) $D_t u(x + t\nu)$ converges in $L^p(\Gamma)$ as $t \to 0-$, for some $1 < p < \infty$, and

iii) $Bu + Tu = h$ on Γ,

where B is a first order differential operator with continuous coefficients, defined in a neighborhood of Γ; T is a bounded operator on $L^p(\Gamma)$; and h is in $L^p(\Gamma)$. In order to apply the theory of [3], we shall assume Γ is of class C_3. Write $Bu = a\partial u/\partial n + Vu$, where a is a continuous function on Γ, and V is a continuous vector field on Γ. Suppose u is any solution of (β), and denote the boundary value $\partial u/\partial n$ by f. Then, by Theorem 2, there is a g in $L^p(\Gamma)$ such that $u(x+t\nu)\to g$ as $t\to 0-$, and $g=J_0(f+Ag)$. Writing ϕ for $f+Ag$, we have $\partial u/\partial n=\phi-A\phi$. Thus in the boundary condition $Bu+Tu=h$ we can replace u by $J_0\phi$, and obtain the equation $a\partial u/\partial n+Vu+Tu=a(\phi-A\phi)+VJ_0\phi+TJ_0\phi=h$. Now it is easy to show (as in [2], Section II D), that VP_0 is a $C_0{}^\infty$ singular integral operator on Γ with symbol $i\{V,\xi/|\xi|\}$, where V is thought of as a cross-section of the tangent bundle of Γ, ξ is a vector in the cotangent bundle of Γ, and $\{\ ,\ \}$ is the bilinear form relating the two. Moreover the operators F, TJ_0, and aA are completely continuous. Thus $H=aI+VP_0+(VP_0F+TJ_0-aA)$ is a $C_0{}^\infty$ singular integral operator with symbol $a+i\{V,\xi/|\xi|\}$; and the solutions u of the problem (β) are isomorphic to the solutions ϕ of the singular integral equation

$$H\phi=h \tag{7}$$

by the isomorphism $u=P(I+F)\phi$.

The difference between the number of orthogonality relations that must be satisfied by h to guarantee a solution of (β), and the dimension of the space of solutions of the associated homogeneous problem: $\Delta u=0$ in G and $Bu+Tu=0$ on Γ, is called the index of the problem (β). We obtain the following result.

THEOREM 3. *If $a+i\{V,\xi/|\xi|\}$ does not vanish at any point on the cotangent bundle of Γ, and the dimension of Γ is $\geqq 2$, then the index of the problem (β) is zero.*

Proof. With these assumptions, Theorem 3 of [3] asserts that the Fredholm alternative holds for the equation (7), and hence for the original boundary value problem. Q. E. D.

Remark 1. The hypothesis of Theorem 3 implies that a is non-vanishing on Γ, i.e. that B is nowhere tangential. If B is real, the condition that $a+i\{V,\xi/|\xi|\}$ vanishes nowhere is equivalent to the condition that B is nowhere tangential

Remark 2. The condition that $a+i\{V,\xi/|\xi|\}$ vanishes nowhere is equivalent to the condition that the boundary operator B covers the Laplacian, in the sense of Schechter (see [1]).

3. The lemmas. In this section $|||T|||$ denotes the supremum for $1\leqq p\leqq\infty$ of the norm of the operator T on $L^p(\Gamma)$. This norm makes the set of operators T for which $|||T|||$ is finite a Banach algebra. The operators P_0 and P_t are described early in Section 1.

LEMMA 1. $|||P_0 - P_t||| \to 0$ *as* $t \to 0$. *If* f *is bounded,* $P_t f \to P_0 f$ *uniformly, and* $P_0 f$ *is continuous.*

Proof. The kernel of $P_0 - P_t$ is $c\,|\mathbf{x} - \mathbf{y}|^{1-k} - c\,|\mathbf{x} + t\boldsymbol{\nu}(\mathbf{x}) - \mathbf{y}|^{1-k} = cQ_t(\mathbf{x},\mathbf{y})$, where $\mathbf{x}$ and $\mathbf{y}$ are points on Γ, and $|\mathbf{x} - \mathbf{y}|$ is the distance from $\mathbf{x}$ to $\mathbf{y}$ in E^{k+1}. Let $\rho(\mathbf{x},\mathbf{y}) = (\mathbf{x} - \mathbf{y})/|\mathbf{x} + t\boldsymbol{\nu} - \mathbf{y}|$ $(\boldsymbol{\nu} = \boldsymbol{\nu}(\mathbf{x}))$. Then a simple argument, based on the fact that $\mathbf{y}$ lies outside the sphere of radius τ about $\mathbf{x} \pm \tau\boldsymbol{\nu}$, shows that $0 \leqq \rho \leqq 2$ for $0 \leqq |t| \leqq \tau$. It follows from this that $|1 - \rho| \leqq 1$, and also $|1 - \rho| \leqq |t|/|\mathbf{x} + t\boldsymbol{\nu} - \mathbf{y}| \leqq 2\,|t|/|\mathbf{x} - \mathbf{y}|$. Thus for the kernel of $P_0 - P_t$ we have $cQ_t(\mathbf{x},\mathbf{y})$, and

$$|Q_t(\mathbf{x},\mathbf{y})| = |\mathbf{x} - \mathbf{y}|^{1-k}\,|1 - \rho^{k-1}| \leqq 2^{k-1}\,|\mathbf{x} - \mathbf{y}|^{1-k}\,|1 - \rho|,$$

or

$$\text{i)} \qquad |Q_t(\mathbf{x},\mathbf{y})| \leqq 2^{k-1}\,|\mathbf{x} - \mathbf{y}|^{1-k} \min\,(1, 2\,|t|/|\mathbf{x} - \mathbf{y}|).$$

Now let $\phi(s)$ be the characteristic function of $0 \leqq s \leqq 1$, and set $R_t(\mathbf{x},\mathbf{y}) = \phi(|\mathbf{x} - \mathbf{y}|\,|t|^{-\frac{1}{2}k})\,Q_t(\mathbf{x},\mathbf{y})$, and $S_t(\mathbf{x},\mathbf{y}) = Q_t(\mathbf{x},\mathbf{y}) - R_t(\mathbf{x},\mathbf{y})$. Then $S_t(\mathbf{x},\mathbf{y})$ vanishes for $|\mathbf{x} - \mathbf{y}| \leqq |t|^{\frac{1}{2}}$, so by (i)

$$|S_t(\mathbf{x},\mathbf{y})| \leqq 2^{k-1}\,|t|\,|\mathbf{x} - \mathbf{y}|^{-k} \leqq 2^{k-1}\,|t|^{\frac{1}{2}},$$

and $S_t(\mathbf{x},\mathbf{y})$ defines an operator S_t with $|||S_t||| = 0(|t|^{\frac{1}{2}})$. Using (i) again, we find that on each coordinate neighborhood $R_t(\mathbf{x},\mathbf{y})$ is dominated by a convolution kernel (in local coordinates), and this dominating kernel comes from a function in $L^1(E^k)$ whose norm is $0(|t|^{1/2k})$. Thus $|||P - P_t||| = 0(|t|^{1/2k})$ as $t \to 0$.

$P_t f$ is continuous for f in $L^1(\Gamma)$ and $t \neq 0$. If f is in L^∞ as well, the above result shows that $P_t f$ converges uniformly to $P_0 f$, and hence that $P_0 f$ is continuous. This establishes Lemma 1.

Remember that D_t denotes differentiation with respect to t.

LEMMA 2. *If* f *is in* $L^p(\Gamma)$, $1 \leqq p < \infty$, *then* $D_t P_t f \to K_0 f + f$ *in* L^p *norm, as* $t \to 0-$, *where* $K_0 f(\mathbf{x}) = \int_\Gamma K_0(\mathbf{x},\mathbf{y}) f(\mathbf{y})\,d\sigma_y$, *and for* $\mathbf{x} \neq \mathbf{y}$ $K_0(\mathbf{x},\mathbf{y}) = D_t c\,|\mathbf{x} + t\boldsymbol{\nu}(\mathbf{x}) - \mathbf{y}|^{1-k}$ *evaluated at* $t = 0$. $K_0(\mathbf{x},\mathbf{y})$ *is uniformly* $0(|\mathbf{x} - \mathbf{y}|^{1-k})$, *and on* $\Gamma \times \Gamma$ *is a continuous function for* $x \neq y$. *If* f *is continuous,* $D_t P_t f$ *converges uniformly to* $K_0 f + f$. *If* f *is bounded,* $K_0 f$ *is continuous.*

Proof. For $t \neq 0$,

$$D_tP_tf(\mathbf{x}) = (1-k)c\int_{\Gamma}(\mathbf{x}+t\boldsymbol{\nu}-\mathbf{y})\cdot\boldsymbol{\nu}\,|\mathbf{x}+t\boldsymbol{\nu}-\mathbf{y}|^{-k-1}f(\mathbf{y})\,d\sigma_y,$$

where $\boldsymbol{\alpha}\cdot\boldsymbol{\beta}$ is the inner product of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ in E^{k+1}. The kernel here is $K_t(\mathbf{x},\mathbf{y})+B_t(\mathbf{x},\mathbf{y})$, with $K_t(\mathbf{x},\mathbf{y}) = (1-k)c(\mathbf{x}-\mathbf{y})\cdot\boldsymbol{\nu}\,|\mathbf{x}+t\boldsymbol{\nu}-\mathbf{y}|^{-k-1}$, and $B_t(\mathbf{x},\mathbf{y}) = (1-k)ct\,|\mathbf{x}+t\boldsymbol{\nu}-\mathbf{y}|^{-k-1}$. Since Γ lies between the spheres of radius τ with centers at $\mathbf{x}\pm\tau\boldsymbol{\nu}$, we have for $\mathbf{x}$ and $\mathbf{y}$ on Γ and $|\mathbf{x}-\mathbf{y}|<\tau$ that $|(\mathbf{x}-\mathbf{y})\cdot\boldsymbol{\nu}| \leqq |\mathbf{x}-\mathbf{y}|^2/\tau$. Thus $K_t(\mathbf{x},\mathbf{y})$ is $0(|\mathbf{x}-\mathbf{y}|^{1-k})$ uniformly in $\mathbf{x}$, $\mathbf{y}$, and t, and an argument like that of Lemma 1 shows that if K_t and K_0 are the operators with kernels $K_t(\mathbf{x},\mathbf{y})$ and $K_0(\mathbf{x},\mathbf{y})$, then $|||K_t-K_0||| \to 0$ as $t\to 0$. As a consequence, if f is bounded then K_0f is continuous, as the uniform limit of the continuous functions K_tf.

We show next that $B_t(\mathbf{x},\mathbf{y})$ satisfies (i): for each $\delta>0$, $B_t(\mathbf{x},\mathbf{y})\to 0$ uniformly in $\mathbf{x}$ and $\mathbf{y}$, for $|\mathbf{x}-\mathbf{y}|>\delta$, as $t\to 0$; and (ii): $\int_{\Gamma}B_t(\mathbf{x},\mathbf{y})\,d\sigma_y\to 1$ uniformly as $t\to 0-$ (and to -1 as $t\to 0+$). Claim (i) is clear, so we turn to (ii). Introduce orthonormal coordinates $(\xi_1,\cdots,\xi_k,\zeta)$ in E^{k+1}, with origin at the point $\mathbf{x}$ in Γ, so that $\zeta=0$ is tangent to Γ at $\mathbf{x}$; and choose α so that $0<\alpha<\tau$, and for $|\mathbf{x}-\mathbf{y}|<\alpha$ Γ can be represented by $\zeta = h(\xi_1,\cdots,\xi_k) = h(\boldsymbol{\xi})$. For simplicity of notation, we let $\boldsymbol{\xi}$ stand for the k-tuple such that $(\boldsymbol{\xi},h(\boldsymbol{\xi})) = (\xi_1,\cdots,\xi_k,h(\boldsymbol{\xi}))$ are the coordinates of the point $\mathbf{y}$ in $\Gamma\cap\{|\mathbf{x}-\mathbf{y}|<\alpha\}$. Then referring again to the two spheres about $\mathbf{x}\pm\tau\boldsymbol{\nu}$, we have the rough estimate

$$\begin{aligned}(\tau-|\boldsymbol{\xi}|)/(\tau+|\boldsymbol{\xi}|) \leqq |\mathbf{x}+t\boldsymbol{\nu}-\mathbf{y}|^2/(|\boldsymbol{\xi}|^2+t^2)&\\ \leqq (\tau+|\boldsymbol{\xi}|)/(\tau-|\boldsymbol{\xi}|),&\end{aligned}$$

where $|\boldsymbol{\xi}|^2=\sum_1^k\xi_i^2$. Also, in $\{|\mathbf{x}-\mathbf{y}|<\alpha\}\cap\Gamma$ we have $d\sigma_y = v_x(\boldsymbol{\xi})\,d\boldsymbol{\xi}$, and $v_x(\boldsymbol{\xi})\to 1$ uniformly in $\mathbf{x}$, as $\boldsymbol{\xi}\to 0$. It is not hard to show that for $t<0$, $(1-k)c\int_{E^k}t(|\boldsymbol{\xi}|^2+t^2)^{-(k+1)/2}d\boldsymbol{\xi} = 1$, and hence that for any $\delta>0$ $(1-k)c\int_{|\xi|<\delta}t(|\boldsymbol{\xi}|^2+t^2)^{-(k+1)/2}d\boldsymbol{\xi}\to 1$, as $t\to 0-$. Thus for any positive $\eta<1$ we can choose a positive $\delta<\alpha$ so that for all $\mathbf{x}$ and $|\boldsymbol{\xi}|<\delta$ we have $\eta^2<|\mathbf{x}+t\boldsymbol{\nu}-\mathbf{y}|^2/(|\boldsymbol{\xi}|^2+t^2)<\eta^{-2}$ and $\eta<v_x(\boldsymbol{\xi})<\eta^{-1}$; and then we can choose $t<0$ so small that $\eta<(1-k)c\int_{|\xi|<\delta}(|\boldsymbol{\xi}|^2+t^2)^{-(k+1)/2}d\boldsymbol{\xi}\leqq 1$. Now let U_x be the neighborhood of $\mathbf{x}$ in Γ projecting onto $|\xi|<\delta$. Then $\int_{\Gamma-U_x}B_t(\mathbf{x},\mathbf{y})\,d\sigma_y\to 0$ uniformly in $\mathbf{x}$ as $t\to 0$; and with $t<0$ we have for

$$\int_{U_\eta} B_t(x,y)\,d\sigma_y = \int_{|\xi|<\delta} (1-k)ct\,|\,x+t\nu-y\,|^{-k-1}v_\eta(\xi)\,d\xi$$

that $\eta^{k+8} < \int_{U_\eta} B_t(x,y)\,d\sigma_y < \eta^{-k-2}$. Thus property (ii) of $B_t(x,y)$ is established.

Now $B_t(x,y)$ is clearly positive for $t<0$, hence has the essential properties of an approximate identity. By a standard argument, $B_t f \to f$ uniformly for any continuous function f. Then another standard argument, relying on the fact that continuous functions are dense in $L^p(\Gamma)$ for $1 \leqq p < \infty$, shows that for f in L^p, $1 \leqq p < \infty$, $B_t f \to f$ in L^p norm. This, together with the results for K_t, establishes Lemma 2.

It is easy to see that $\lim\limits_{t\to 0+} D_t P_t f = -f + K_0 f$. This with Lemma 2 is a formulation of the "jump" relations for the adjoint of the double layer potential.

Lemma 3. *If J^t is the operator on $L^p(\Gamma)$ $(1 \leqq p \leqq \infty)$ defined by the krenel* (5), *then for each p $\| J^t - J_0 \| \to 0$ as $t \to 0$.*

Proof. With reference to the kernels defined in (2), set

$$L^t(x,y) = L_t(x',y')v_t(y), \qquad F^t(x,y) = F_t(x',y')v_t(y),$$

$$\text{and } P^t(x,y) = c\,|\,x'-y'\,|^{1-k}v_t(y),$$

where $x' = x + t\nu(x)$, $y' = y + t\nu(y)$, and

$$\int_{\Gamma_t} \phi(y')\,d\sigma_{y'} = \int_\Gamma \phi(y + t\nu(y))\,v_t(y)\,d\sigma_y$$

for continuous ϕ. Then

$$F^t(x,y) = -L^t(x,y) - \int_\Gamma L^t(x,z)F^t(z,y)\,d\sigma_z$$

and $J^t(x,y) = P^t(x,y) + \int_\Gamma P^t(x,z)F^t(z,y)\,d\sigma_z$. We will achieve the desired result by showing in turn that $|||\,P^t - P_0\,||| \to 0$, $|||\,L^t - L\,||| \to 0$, $\| F^t - F \|_p \to 0$, and finally $\| J^t - J_0 \|_p \to 0$. The first two cases are quite similar, and we discuss only $P^t - P_0$. The kernel of this operator is $c\{|\,x'-y'\,|^{1-k}v_t(y) - |\,x-y\,|^{1-k}\}$, which is $0(|x-y|^{1-k})$ uniformly in x, y, and t, and for $|\,x-y\,| \geqq \delta > 0$ converges uniformly to 0. Hence for any $\epsilon > 0$ we can choose $\delta > 0$ so that restricting the kernel to $|\,x-y\,| \leqq \delta$ yields an operator whose norm on $L^p(\Gamma)$, for all $1 \leqq p \leqq \infty$, is $< \epsilon/2$. We can then choose $t_0 > 0$ so that, for $|\,t\,| < t_0$, restricting the kernel to $|\,x-y\,| \geqq \delta$ yields an operator whose norm on L^p, for all $1 \leqq p \leqq \infty$, is $< \epsilon/2$. Thus for $|t| < t_0$, $|||P^t - P_0||| < \epsilon$. In the same way, $|||L^t - L_0||| \to 0$ as $t \to 0$.

Since $I + L$ has trivial null space, and L is completely continuous on $L^p(\Gamma)$, $\phi + L\phi = \psi$ has a unique solution ϕ for each ψ in $L^p(\Gamma)$, i.e. $I + L$ is one to one and onto. For any fixed p in $1 \leqq p \leqq \infty$, it follows from the complete continuity of L that the inf $\| \phi + L\phi \|_p$ for $\| \phi \|_p = 1$ is not zero; for if $\| \phi_n \|_p = 1$ and $\phi_n + L\phi_n \to 0$, we can choose a subsequence ϕ'_n with $L\phi'_n$ convergent, from which it follows that for some ϕ $\phi'_n \to \phi$, with $\| \phi \|_p = 1$ and $\phi + L\phi = 0$. This contradicts the fact that $I + L$ has trivial null space. Thus $I + L$ has a bounded inverse and hence for sufficiently small t, $I + L^t$ has a bounded inverse that converges (in L^p operator norm) to $(I + L)^{-1}$, as $t \to 0$. Then $F^t = -(I + L^t)^{-1}L^t$ converges to $F = -(I + L)^{-1}$, and $J^t = p^t(I + F^t)$ converges to $J_0 = P_0(I + F)$, as required in the statement of the lemma.

REFERENCES.

[1] Martin Schechter, "Integral inequalities for partial differential equations satisfying general boundary conditions," *Communications on Pure and Applied Mathematics*, vol. 12 (1959), pp. 37-66.

[2] R. T. Seeley, "Singular integrals on compact manifolds," *American Journal of Mathematics*, vol. 81 (1959), pp. 658-690.

[3] ———, "Regularization of singular integral operators on compact manifolds," *American Journal of Mathematics*, vol. 83 (1961), pp. 265-275.

AFFINE RINGS OVER RANK TWO REGULAR LOCAL RINGS.

By Louis J. Ratliff, Jr.

---

1. **Introduction.** An integral domain $\mathfrak{o}$ is an *affine ring* over a domain I in case I is a Noetherian domain and $\mathfrak{o}$ is finitely generated ov If $\mathfrak{o}$ is an affine ring over I and if $\mathfrak{p}$ is a prime ideal in $\mathfrak{o}$, then the quotient $P = \mathfrak{o}_{\mathfrak{p}}$ of $\mathfrak{o}$ with respect to $\mathfrak{p}$ is said to be a *spot* over I, hence a spot P (Noetherian) local domain. If the completion (relative to the powers o product of the maximal ideals) of a (Noetherian) semi-local domai contains no nonzero nilpotent elements, then P is said to be *analyti unramified.*

A Noetherian domain I is said to satisfy the *condition* (SF) if separably generated affine ring $\mathfrak{o}$ over I is such that the integral closure in its quotient field is a finite $\mathfrak{o}$-module. It is well known ([9], p. 267) a field satisfies the condition (SF), and recently Nagata ([4], p. 419) proven that a Dedekind domain satisfies this condition. Nagata's pro essentially based on the following two facts.

1.1. Let $\mathfrak{o}$ be an affine ring over I, and let $\mathfrak{o}^*$ be an integral do which contains $\mathfrak{o}$ and is a finite $\mathfrak{o}$-module. If $\mathfrak{p}^*$ is a prime ideal in $\mathfrak{o}^*$, rank $\mathfrak{p}^* =$ rank $(\mathfrak{p}^* \cap \mathfrak{o})$.

1.2. If P is a separably generated spot over I, then the integral cl of P in its quotient field is a finite P-module ([4], p. 417).

It is known ([4], p. 414) that if a local domain P is analytically ramified, then the integral closure of P in its quotient field is a P-module. Hence statement 1.2 above is a consequence of

1.3. If P is a spot which is separably generated over I, then analytically unramified ([4], p. 416).

In this paper, generalizing the methods of Nagata [3, 4], it is p that statements 1.1 and 1.3 remain valid if I is a rank two regular ring which has an infinite residue field, and as a consequence it is p

---

* Received August 8, 1961.

[1] This paper was written while the writer held a National Science Foundatio operative Fellowship, and constitutes the main results of his doctoral dissertatio

that a rank two regular local ring which has an infinite residue field satisfies the condition (SF).

For the remainder of this section the letter I will denote a rank two regular local ring which has an infinite residue field.

Section 2 contains the definitions of most of the terms used in this paper. By employing some results of Nagata [5, 6] it is proven in Section 3 that if $\mathfrak{o}$ is an affine ring over I and if $\mathfrak{q}$ is a maximal ideal in $\mathfrak{o}$, then the transcendence degree of $\mathfrak{o}$ over I is equal to the rank of $\mathfrak{q}$ minus the rank of $\mathfrak{q} \cap I$ (in symbols, $\operatorname{trd}(\mathfrak{o}/I) = \operatorname{rank} \mathfrak{q} - \operatorname{rank}(\mathfrak{q} \cap I)$). Several corollaries to this theorem which are needed in Section 4 are then proven, and Corollary 2 is the generalization of statement 1.1 above to the case where I is a rank two regular local ring. In Section 4 it is proven that statement 1.3 above remains true when I is a rank two regular local ring which has an infinite residue field. The proof is broken into three parts. Namely, let P be a spot which is separably generated over I. If P does not dominate I, then P is a spot which is separably generated over a Dedekind domain or a field, hence P is analytically unramified by Nagata's result mentioned in 1.3 above. Secondly, if P dominates I and contains a set of elements which has a certain property ("property (T)") defined below, then by means of a finite number of quadratic transforms of I it is shown that P is a subspace of a semi-local domain P^* such that, if M^* is a maximal ideal in P^*, then $P^*_{M^*}$ is a spot which is separably generated over a Dedekind domain. Hence, by certain well known theorems on completions of a semi-local domain ([10], pp. 277, 283), P is analytically unramified. Finally, if P dominates I and does not contain a set of elements which has the property (T), then it is necessary to derive some information concerning the structure of such a spot (Remark 4.2 and Lemma 4.5). These structure theorems are generalizations of two theorems ([3], p. 86, and [4], p. 397) due to Nagata, and are used to show that there is imbedded in P a semi-local domain D such that P is a spot over D and D has the same quotient field as P. Then by using a recent result due to Rees [8] it is seen that P is analytically unramified by proving that D is analytically unramified. Having proven that every spot P which is separably generated over I is analytically unramified, it follows that the integral closure of P in its quotient field is a finite P-module ([4], p. 414), and then Nagata's proof that a Dedekind domain has the property (SF) carries over verbatim to prove that a rank two regular local ring which has an infinite residue field has the property (SF).

The author expresses his gratitude to Professor H. T. Muhly for his encouragement and many helpful suggestions.

2. Definitions and notation.

All rings in this paper are assumed to be commutative rings with a unit element 1.

A ring $\mathfrak{o}$ has *rank* r in case there exists a chain

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r \tag{2.1}$$

of $r+1$ proper prime ideals $\mathfrak{p}_i$ in $\mathfrak{o}$, and there does not exist such a chain with more than $r+1$ prime ideals. (The symbol $\subset$ is used to indicate *proper* inclusion). If $\mathfrak{p}$ is a prime ideal in $\mathfrak{o}$, then the *rank* of $\mathfrak{p}$ is the rank of $\mathfrak{o}_{\mathfrak{p}}$, and if $\mathfrak{a}$ is an ideal in $\mathfrak{o}$, then the *rank* of $\mathfrak{a}$ is the minimum of the ranks of the prime divisors of $\mathfrak{a}$. A chain (2.1) of prime ideals in an integral domain $\mathfrak{o}$ is a *maximal chain* of prime ideals in $\mathfrak{o}$ in case the rank of $\mathfrak{p}_i/\mathfrak{p}_{i-1}$ is one $(i=1,\cdots,r)$, $\mathfrak{p}_0=(0)$, and $\mathfrak{p}_r$ is a maximal ideal in $\mathfrak{o}$. The *length* of the chain is r.

Let $\mathfrak{o}$ be an integral domain. The integral closure $\mathfrak{o}'$ of $\mathfrak{o}$ in its quotient field is the *derived normal ring* of $\mathfrak{o}$, and $\mathfrak{o}$ is said to be *normal* in case $\mathfrak{o}$ is equal to $\mathfrak{o}'$.

If a ring P has only one maximal ideal M, then this fact will often be displayed by the notation (P,M), and it is said that (P,M) is a *quasi-local ring*. Let (P,M) and (Q,N) be two quasi-local rings. Then P *dominates* $Q (P \geqq Q)$ in case $P \supseteq Q$ and $M \cap Q = N$. If a quasi-local ring P is a Noetherian ring, then P is called a *local ring*. A Noetherian ring P which has only a finite number of maximal ideals is called a *semi-local ring*.

Remark 2.1. Let P, Q, and R be local rings such that P is a spot over Q which dominates Q, and Q is a spot over R which dominates R. Then P is a spot over R which dominates R.

Let (P,M) be a local ring, let $y_1,\cdots,y_t$ be algebraically independent over P, and let $R=P[y_1,\cdots,y_t]$. Then the ring R_{MR} will be denoted by $P(y_1,\cdots,y_t)$.

A ring I is a *ground ring* in case I is a field, a Dedekind domain, or a rank two regular local ring which has an infinite residue field. The theorems which will be proven in this paper are known [3, 4] if the ground ring is a field or a Dedekind domain. Therefore *all future statements in this paper concerning a ground ring I are to be interpreted as statements about a rank two regular local ring which has infinitely many elements in its residue field.*

Let (P,M) be a spot over a ground ring (I,m). A ring B contained in P is said to be a *basic ring* in P in case 1) P is a spot over B, and B is a spot over I, 2) $P \geqq B$, and $B \geqq I_{(M\cap I)}$, 3) B is a field, a Dedekind domain, or a ground ring, and 4) P/M is a finite algebraic extension of $B/(M\cap B)$.

Remark 2.2. Let (P, M) be a spot over a ground ring (I, m). If P contains a basic ring (B, N), then P is a quotient ring with respect to a *maximal* ideal of an affine ring over B.

Proof. By the definition of a basic ring $P = A_{\mathfrak{q}}$, where $A = B[b_1, \cdots, b_n]$ and $\mathfrak{q}$ is a prime ideal in A. Suppose that $\mathfrak{q}$ is *properly* contained in $\mathfrak{q}^*$, where $\mathfrak{q}^*$ is a maximal ideal in A. Since $P \geqq B$, $\mathfrak{q} \cap B = N$, and since $\mathfrak{q}^* \supset \mathfrak{q}$, $\mathfrak{q}^* \cap B = N$. Hence the natural homomorphism of $(B/N)[b_1', \cdots, b_n']$ onto $(B/N)[b_1^*, \cdots, b_n^*]$ has a nonzero kernel, where b_i' and b_i^* are the residue classes of b_i modulo $\mathfrak{q}$ and $\mathfrak{q}^*$ respectively. Therefore $\operatorname{trd}((A/\mathfrak{q})/(B/N)) > \operatorname{trd}((A/\mathfrak{q}^*)/(B/N))$. But B is a basic ring in P and P/M is isomorphic to the quotient field of $A/\mathfrak{q}$, so $\operatorname{trd}((A/\mathfrak{q})/(B/N)) = \operatorname{trd}((P/M)/(B/N)) = 0$, hence $\operatorname{trd}((A/\mathfrak{q}^*)/(B/N)) < 0$, contradiction. Hence $\mathfrak{q}$ is a maximal ideal in A, q. e. d.

Let (R, N) be a local domain, and let (S, M) be a spot over R which dominates R. Then R satisfies the *dimension formula* in case

$$(2.2) \qquad \operatorname{rank} S + \operatorname{trd}((S/M)/(R/N)) = \operatorname{rank} R + \operatorname{trd}(S/R).$$

An integral domain R satisfies the *first chain condition* in case every maximal chain of prime ideals in R has length equal to the rank of R. R satisfies the *second chain condition* in case every integral domain which contains R and is integrally dependent on R satisfies the first chain condition.

A *derivation* D of an integral domain S is an additive endomorphism of the quotient field K of S which satisfies the conditions 1) $D(xy) = xDy + yDx$, for all $x, y \in K$, and 2) there exists an element d in S such that $dDx \in S$, for all $x \in S$. If $Da = 0$ for every element a in a subdomain R of S, then D is said to be a *derivation of S over R*.

3. The rank of an affine ring over a ground ring. As stated in Section 2 the statement that I is a ground ring is to mean that I is a rank two regular local ring which has an infinite residue field. However, the assumption that the residue field of a ground ring I is infinite is not needed in this section.

Nagata [5, 6] has proven two theorems which are stated as Remark 3.1 for future reference.

Remark 3.1. The second chain condition holds in a Noetherian domain I if and only if the first chain condition holds in the derived normal ring of I. Further, if I satisfies the second chain condition, and if P is a spot over I, then P satisfies the second chain condition and the dimension formula.

LEMMA 3.1. *Let* (I, m) *be a ground ring, and let* $\mathfrak{p}$ *be a prime ideal in* I. *Then* $I_{\mathfrak{p}}$ *satisfies the dimension formula and the second chain condition.*

Proof. Since $(0) \subset m$ is not a maximal chain of prime ideals in I, I satisfies the first chain condition. Since I is a normal Noetherian domain ([10], p. 302), I satisfies the second chain condition (Remark 3.1). Since $I_{\mathfrak{p}}$ is a spot over I, $I_{\mathfrak{p}}$ satisfies the dimension formula and the second chain condition (Remark 3.1), q. e. d.

THEOREM 3.1. *Let* $\mathfrak{o} = I[z_1, \cdots, z_n]$ *be an affine ring over a ground ring* (I, m), *let* $\mathfrak{q}$ *be a maximal ideal in* $\mathfrak{o}$, *and let* $\mathfrak{q} \cap I = \mathfrak{p}$. *Then* $\operatorname{trd}(\mathfrak{o}/I) = \operatorname{rank}\mathfrak{q} - \operatorname{rank}\mathfrak{p}$.

Remark. It is not difficult to show that there does not exist a maximal ideal $\mathfrak{q}$ in $\mathfrak{o}$ such that $\mathfrak{q} \cap I = (0)$. Hence, if $\mathfrak{q}$ is a maximal ideal in $\mathfrak{o}$, then $\operatorname{rank}\mathfrak{q} = r + 1$ or $r + 2$, where $r = \operatorname{trd}(\mathfrak{o}/I)$. Since no use is made of this fact in the remainder of this paper, the proof that $\mathfrak{q} \cap I \neq (0)$ will not be given.

Proof of Theorem 3.1. Set $P = \mathfrak{o}_{\mathfrak{q}}$ and $M = \mathfrak{q}P$, so (P, M) is a spot over $I_{\mathfrak{p}}$. Since $I_{\mathfrak{p}}$ satisfies the second chain condition (Lemma 3.1), every maximal chain of prime ideals in P has length equal to the rank of P (Remark 3.1), hence equal to the rank of M. Since there is a one to one correspondence between the prime ideals in $\mathfrak{o}$ which are contained in $\mathfrak{q}$ and the prime ideals in P, every maximal chain of prime ideals in $\mathfrak{o}$ which ends at $\mathfrak{q}$ has length equal to the rank of $\mathfrak{q}$. By Remark 3.1 $I_{\mathfrak{p}}$ satisfies the dimension formula (2.2), so $\operatorname{rank}P + \operatorname{trd}((\mathfrak{o}/\mathfrak{q})/(I/\mathfrak{p})) = \operatorname{rank}I_{\mathfrak{p}} + \operatorname{trd}(\mathfrak{o}/I)$, since $\operatorname{trd}((P/M)/(I_{\mathfrak{p}}/\mathfrak{p}I_{\mathfrak{p}})) = \operatorname{trd}((\mathfrak{o}/\mathfrak{q})/(I/\mathfrak{p}))$, and $\operatorname{trd}(\mathfrak{o}/I) = \operatorname{trd}(P/I_{\mathfrak{p}})$. Further, $\mathfrak{o}$ is finitely generated over I and $\mathfrak{q}$ is a maximal ideal in $\mathfrak{o}$, hence $\operatorname{trd}((\mathfrak{o}/\mathfrak{q})/(I/\mathfrak{p})) = 0$. Therefore

$$\operatorname{trd}(\mathfrak{o}/I) = \operatorname{rank}P - \operatorname{rank}I_{\mathfrak{p}} = \operatorname{rank}\mathfrak{q} - \operatorname{rank}\mathfrak{p},$$

q. e. d.

COROLLARY 3.1. *With the same notation as in Theorem* 3.1, *if* $(0) = \mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_s = \mathfrak{q}$ *is a maximal chain of prime ideals in* $\mathfrak{o}$, *then* $s = \operatorname{rank}\mathfrak{q}$.

Proof. Proved in the course of proving Theorem 3.1.

COROLLARY 3.2. *Let* $\mathfrak{o}$ *be an affine ring over a ground ring* I, *let* $\mathfrak{o}^*$ *be an integral domain which contains* $\mathfrak{o}$ *and is a finite* $\mathfrak{o}$ *module, and let* $\mathfrak{p}^*$ *be a prime ideal in* $\mathfrak{o}^*$. *Then* $\operatorname{rank}\mathfrak{p}^* = \operatorname{rank}(\mathfrak{p}^* \cap \mathfrak{o})$.

Proof. Consider a maximal chain of prime ideals through $\mathfrak{p}^*$ in $\mathfrak{o}^*$ ending at, say, $\mathfrak{q}^*$. The length of this chain is equal to the rank of $\mathfrak{q}^*$ (Corollary 3.1). Since $\mathfrak{o}^*$ is integrally dependent on $\mathfrak{o}$, the contraction in $\mathfrak{o}$ of the ideals in this chain yields a chain of distinct prime ideals in $\mathfrak{o}$, and $\mathfrak{q}^* \cap \mathfrak{o}$ is a maximal ideal in $\mathfrak{o}$. Clearly $\mathrm{trd}(\mathfrak{o}^*/I) = \mathrm{trd}(\mathfrak{o}/I)$, and $\mathfrak{q}^* \cap I = (\mathfrak{q}^* \cap \mathfrak{o}) \cap I$, so $\mathrm{rank}(\mathfrak{q}^* \cap I) = \mathrm{rank}((\mathfrak{q}^* \cap \mathfrak{o}) \cap I)$, hence $\mathrm{rank}\,\mathfrak{q}^* = \mathrm{rank}(\mathfrak{q}^* \cap \mathfrak{o})$ (Theorem 3.1). Since the contracted chain of prime ideals has length equal to the rank of $\mathfrak{q}^*$, it has length equal to the rank of $\mathfrak{q}^* \cap \mathfrak{o}$, hence it is a maximal chain of prime ideals in $\mathfrak{o}$. Therefore $\mathrm{rank}(\mathfrak{p}^* \cap \mathfrak{o}) = \mathrm{rank}\,\mathfrak{p}^*$, q. e. d.

COROLLARY 3.3. *Let (P, M) be a spot over a ground ring I, let $A = P[\theta_1, \cdots, \theta_k]$ be a finite P-module, and let $\mathfrak{p}$ be a prime ideal in A. Then* $\mathrm{rank}\,\mathfrak{p} = \mathrm{rank}(\mathfrak{p} \cap P)$.

Proof. Let Q be a maximal ideal in A which contains $\mathfrak{p}$, and let $P = \mathfrak{o}_{\mathfrak{q}}$, where $\mathfrak{q}$ is a prime ideal in $\mathfrak{o} = I[z]$ $(= I[z_1, \cdots, z_n])$. Since A is a finite P-module, each θ_i is integrally dependent on P, hence there exist elements $r_i \in \mathfrak{o}$, $r_i \notin \mathfrak{q}$, such that the elements $r_i\theta_i$ are integrally dependent on $\mathfrak{o}$. Set $S = \mathfrak{o}[r\theta]$, so S is a finite $\mathfrak{o}$-module. Clearly $A \supseteq S$, so

$$A_Q \geqq S_{(Q \cap S)} \geqq \mathfrak{o}_{(Q \cap \mathfrak{o})} = \mathfrak{o}_{\mathfrak{q}} = P,$$

hence $S_{(Q \cap S)} \supseteq A$, since the elements $r_i \notin Q \cap S$. Therefore $A_Q = S_{(Q \cap S)}$. Since S is a finite $\mathfrak{o}$-module, and since $(\mathfrak{p} \cap S) \cap \mathfrak{o} = (\mathfrak{p} \cap P) \cap \mathfrak{o}$, $\mathrm{rank}(\mathfrak{p} \cap S) = \mathrm{rank}((\mathfrak{p} \cap P_1) \cap \mathfrak{o})$ (Corollary 3.2). Since A_Q and P are quotient rings of S and $\mathfrak{o}$ respectively, $\mathrm{rank}(\mathfrak{p} \cap S) = \mathrm{rank}\,\mathfrak{p}$, and $\mathrm{rank}((\mathfrak{p} \cap P) \cap \mathfrak{o} = \mathrm{rank}(\mathfrak{p} \cap P)$, q. e. d.

COROLLARY 3.4. *Let (P, M) be a spot over a ground ring I. Assume that P contains a basic ring (B, M), where B is a rank two regular local ring which dominates I. Then* $\mathrm{rank}\,P = \mathrm{trd}(P/B) + 2$.

Proof. By Remark 2.2 P is a quotient ring with respect to a maximal ideal of an affine ring over B. Since B is a ground ring, and since $\mathrm{rank}(M \cap B) = \mathrm{rank}\,N = 2$, $\mathrm{rank}\,P = \mathrm{trd}(P/B) + 2$ (Theorem 3.1), q. e. d.

4. Analytical unramifiedness of spots which are separably generated over a ground ring. The main part of this section is devoted to proving

THEOREM 4.1. *If (P, M) is a spot which is separably generated over a ground ring (I, m), then P is analytically unramified.*

The proof of this theorem is attained by combining propositions 4.1, 4.2, and 4.3 below.

PROPOSITION 4.1. *Let (P, M) be a spot which is separably generated over (I, m). If P does not dominate I, then P is analytically unramified.*

Proof. Since P does not dominate I, the rank of $M \cap I$ is one or zero. Since a quotient ring with respect to a prime ideal of a regular local ring is a regular local ring ([7], p. 208), and since a rank one regular local ring is a local Dedekind domain, if rank $M \cap I = 1$, then $I_{(M \cap I)}$ is a local Dedekind domain, and if $M \cap I = (0)$, then $I_{(M \cap I)}$ is a field. Therefore P is a spot which is separably generated over a Dedekind domain or a field, hence P is analytically unramified ([4], p. 416), q. e. d.

Henceforth *the statement that P is a spot over I will mean that P is a spot which is separably generated over a ground ring I and which dominates I.* Further, *the letter t will consistently be used to denote the transcendence degree of P/M over I/m.*

Definition 4.1. Let (P, M) be a spot over (I, m). A set of t elements $y_1, \cdots, y_t$ in P is said to have the *property* (T) in case the residues of the y_i modulo M are a transcendence base for P/M over I/m, and the y_i are algebraically dependent over I.

Definition 4.2. Let (P, M) be a spot over (I, m). If P contains a set of element which has the property (T), then P is said to be a spot of *type one.* P is a spot of *type two* in case P is not a spot of type one.

COROLLARY 4.1. *If (P, M) is a rank one spot over (I, m), then P is a spot of type one.*

Remark. There exist rank one spots which dominate I. For example, let $m = (a, b)I$, let $R = I[b/a]$, and let $\mathfrak{p}$ be a rank one prime divisor of aR. Then $R_{\mathfrak{p}}$ is a rank one spot which dominates I.

Proof of Corollary 4.1. By Remark 3.1 I satisfies the dimension formula (2.2), so $t = \operatorname{trd}((P/M)/(I/m)) = 1 + \operatorname{trd}(P/I)$, hence every set of elements in P whose residues modulo M are a transcendence base for P/M over I/m is a set of element which has the property (T), hence P is a spot of type one, q. e. d.

LEMMA 4.1. *Let (P, M) be a spot of type one over (I, m), let $y_1, \cdots, y_t$ be a set of elements in P which has the property (T), and let $S = I[y_1, \cdots, y_t]$. Then mS is a prime ideal in S, and P dominates S_{mS}.*

Proof. Let $P = \mathfrak{o}_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal in $\mathfrak{o} = I[z]$ $(= I[z_1, \cdots, z_n])$. Let σ be the restriction to S of the natural homomorphism from P onto P/M. Since $P \geqq I$, P/M is isomorphic to $(I/m)(z_1', \cdots, z_n')$, $S/(M \cap S)$ is isomorphic to $(I/m)[y_1', \cdots, y_t']$ (the $'$ indicates residues modulo M), and $\ker \sigma = M \cap S \supseteq mS$. Conversely, if $f(y)$ is in $\ker \sigma$, then all coefficients of f are in m, since the y_i' are algebraically independent over I/m. Thus $\ker \sigma = mS$, so mS is a prime ideal, hence $P \geqq S_{(M \cap S)} = S_{mS}$, q. e. d.

LEMMA 4.2. *Let (P, M) be a spot over (I, m), let P' be the derived normal ring of P, let $M_1', \cdots, M_h'$ be the totality of maximal ideals in P', let θ_i be elements in P' such that $\theta_i \equiv \delta_{ij}$ (M_j') $(i, j = 1, \cdots, h)$, and let $A = P[\theta_1, \cdots, \theta_h]$. Then A is a semi-local domain which has exactly h maximal ideals $Q_i = M_i' \cap A$. Let $P_i = A_{Q_i}$. Then the derived normal ring P_i' of P_i is $P'_{M_i'}$.*

Remark. The fact that P' has only a finite number of maximal ideals is proven in [2].

Proof. Set $Q_i = M_i' \cap A$. Since A is integrally dependent on P, the derived normal ring A' of A is equal to P', hence each Q_i is a maximal ideal in A, and the Q_i are distinct by the choice of the θ_i. Therefore there exist at least h maximal ideals in A. If Q is an arbitrary maximal ideal in A, then there exists a maximal ideal M' in P' such that $M' \cap A = Q$, since P' is integrally dependent on A. Since M' is one of the M_i', $Q = M_i' \cap A = Q_i$. Thus there exist exactly h maximal ideals in A. Also A is Noetherian, since P is Noetherian, hence A is a semi-local domain. Fix i and set $R = P'_{M_i'}$, $N = M_i'R$, and $\mathfrak{p} = N \cap P_i'$ (R contains P_i', since R is normal). Then $R \geqq (P_i')_{\mathfrak{p}}$. If $\mathfrak{q}$ is a maximal ideal in P_i', then $\mathfrak{q} \cap A' = \mathfrak{q} \cap P' = M_i'$, so $(P_i')_{\mathfrak{q}} \geqq R \geqq (P_i')_{\mathfrak{p}}$, hence $\mathfrak{p} = \mathfrak{q}$, and $P_i' = (P_i')_{\mathfrak{p}} = R$, q. e. d.

Remark 4.1. With the same notation as in Lemma 4.2, if $d_1, \cdots, d_k$ are elements in P_i', then $S = P_i[d_1, \cdots, d_k]$ is a *spot* over I, and $\operatorname{rank} S = \operatorname{rank} P$. Further, $\operatorname{trd}((S/Q)/(I/m)) = \operatorname{trd}((P_i/M_i)/(I/m))$, where Q and M_i are the unique maximal ideals in S and P_i respectively.

Proof. The proof that S is a spot over I follows from Remark 2.1 and the fact that P_i' is a quasi-local domain, and $\operatorname{rank} S = \operatorname{rank} P$ by Corollary 3.3. The last statement is clear, since the d_j are integrally dependent on P_i.

LEMMA 4.3. *Let (P, M) be a spot of type one over (I, m). There exists a semi-local domain P^* which is contained in the derived normal ring* *of P such that* 1) *P^* contains P and is a finite P-module, and* 2) *if M^* is a maximal ideal in P^*, then $P^*_{M^*}$ is a spot which is separably generated over a Dedekind domain.*

Proof. Let P' be the derived normal ring of P, and in the notation of Lemma 4.2 let $A = P[\theta_1, \cdots, \theta_h]$. Then by Lemma 4.2 A is a semi-local domain which has h maximal ideals $Q_i = M_i' \cap A$, P_i' is a quasi-local domain, and by Remark 4.1 P_i is a spot over I $(i = 1, \cdots, h)$. Let $y_1, \cdots, y_t$ be a set of elements in P which has the property (T). Since the θ_i are integrally dependent on P, it is clear that $y_1, \cdots, y_t$ are elements in P_i which form a set which has the property (T). Further, if an element d is in the derived normal ring of P_j, then there exists an element $r \in A$, $r \notin Q_j$ such that rd is an element in the derived normal ring of A. Hence, in view of Remark 4.1 it is sufficient to prove the lemma in the case where the derived normal ring of P is a quasi-local domain (and in this case the ring P^* is a *local* domain).

Let L and F be the quotient fields of P and I respectively, let (R_v, M_v) be the valuation ring of a real discrete valuation v of L such that $R_v \geqq P$ (existence of R_v is proven in [1]), let w be the restriction of v to F, and let (T_w, N_w) be the valuation ring of w. Then clearly $T_w \geqq I$, hence w is not trivial on F. Let $Y_1, \cdots, Y_t$ be indeterminants, and extend w to $I[Y]$ $(= I[Y_1, \cdots, Y_t])$ by defining $w(g(Y)) = \min\{w(r_i);\ r_i$ is a coefficient of $g(Y)\}$. Since $y_1, \cdots, y_t$ are elements in P which form a set which has the property (T), there exist polynomials $f(Y)$ in $I[Y]$ such that $f(y) = 0$ and reducing modulo M the equation $f(y) = 0$ it is seen that all coefficients of $f(Y)$ are in m. Among the polynomials $f(Y)$ such that $f(y) = 0$ let $g(Y)$ be such that $w(g(Y))$ is a minimum (such a polynomial exists since $T_w \geqq I$). Let $g(Y) = \sum r_i M_i(Y)$, where $M_i(Y)$ is a monomial with a coefficient which is a unit in I. Then $w(g(Y)) > 0$, so it may be assumed tat each $r_i \in m^\beta$, and that at least one $r_i \notin m^{\beta+1}$. Let $m = (a, b)I$. Then $r_i = \sum r_{ij} a^{\beta-j} b^j$, and since at least one $r_i \notin m^{\beta+1}$, at least one r_{ij} is a unit in I. Set $\phi_j(Y) = \sum r_{ij} M_i(Y)$, so $g(Y) = \sum \phi_j(Y) a^{\beta-j} b^j$. Further, $w(\phi_j(Y)) = 0$, for some j, hence $\phi_j(y) \neq 0$.

Under the unimodular transformation $b_1 = b$, $a_1 = a - cb_1$, where c is a unit in I, the coefficient of $b_1{}^\beta$ in $g(Y)$ is $\sum \phi_j(Y) c^{\beta-j}$. Since I/m is an infinite field, there exist values of c such that the coefficient of $b_1{}^\beta$ $(= \sum_i (\sum_j r_{ij} c^{\beta-j}) M_i(Y))$, is such that for at least one i $\sum r_{ij} c^{\beta-j}$ is a unit in I, hence $\sum \phi_j(y) c^{\beta-j} \neq 0$. Thus it may be assumed that the coefficient $\phi_\beta(Y)$ of b^β in $g(Y)$ has the property that $w(\phi_\beta(Y)) = 0$, hence $\phi_\beta(Y)$ has a coefficient which is a unit in I. Therefore $\phi_\beta(y)$ is a unit in S_{mS}, where

$S = I[y_1, \cdots, y_t]$ (mS is a prime ideal by Lemma 4.1). By Lemma 4.1 $P \geqq S_{mS}$, hence $\phi_\beta(y)$ is a unit in P. Hence, from

$$0 = g(y) = \phi_\beta(y) b^\beta + \phi_{\beta-1}(y) b^{\beta-1} a + \cdots + \phi_0(y) a^\beta,$$

it is seen that b/a is integrally dependent on P.

Set $P_0 = P$, $P_1 = P_0[b/a]$, and let M_1 be the maximal ideal in P_1. Since P' is a quasi-local domain, P_1 is a *local* domain contained in P' which is a finite P-module and which dominates P. Set $I_0 = I$, $J = I_0[b/a]$, $I_1 = J_{(M_1 \cap J)} = J_{(N_w \cap J)}$, and $m_1 = (M_1 \cap J) I_1$. Then (P_1, M_1) is a spot (which is separably generated) over (I_1, m_1), and $P_1 \geqq I_1$. (I_1 is called the *first quadratic transform* of I along w. It is known ([4], p. 404) that I_1 is a regular local ring which dominates I, and rank $I_1 \leqq$ rank I. Let I_k be the first quadratic transform of I_{k-1} ($k \geqq 1$) along w (assuming rank $I_{k-1} > 1$). Then I_k is called the *k-th quadratic transform* of I along w). If rank $I_1 = 1$, then the theorem is proved. If rank $I_1 = 2$, then $y_1, \cdots, y_t$ are elements in P_1 which form a set with the property (T), $R_v \geqq P_1$, $T_w \geqq I_1$, and the derived normal ring of P_1 is P', so the above process can be repeated. Let $g_1(Y)$ be an element in $I_1[Y]$ such that $g_1(y) = 0$ and $w(g_1(Y))$ is a minimum. Then $w(g_1(Y)) > 0$. Since $r_i \in m^\beta \subseteq a^\beta I_1$, $r_i = a^\beta \mu_i$, where $\mu_i \in I_1$, so $g(Y) = a^\beta f(Y)$, where $f(Y) = \sum \mu_i M_i(Y)$. Since $g(y) = 0$, $f(y) = 0$, hence $w(g(Y)) > w(f(Y)) \geqq w(g_1(Y)) > 0$. Since $w(g(Y))$ is an integer, in a finite number of steps, say k, rank $I_k = 1$, where I_k is the k-th quadratic transform of I along w, and P_k is a spot (which is separably generated) over I_k. Since I_k is a regular local ring of rank one, I_k is a local Dedekind domain, q. e. d.

PROPOSITION 4.2. *Let (P, M) be a spot over (I, m). If P is a spot of type one, then P is analytically unramified.*

Proof. Let P^* be the semi-local domain constructed in Lemma 4.3, and let M^* be a maximal ideal in P^*. Then $P^*_{M^*}$ is a spot which is separably generated over a Dedekind domain, hence $P^*_{M^*}$ is analytically unramified ([4], p. 416). Since the completion of P^* is isomorphic to the direct sum of the completions of the $P^*_{M^*}$ ([10], p. 283), P^* is analytically unramified Since P^* is an integral domain which is a finite P-module (Lemma 4.3), the completion of P is a subring of the completion of P^* ([10], p. 277), hence P is analytically unramified, q. e. d.

COROLLARY 4.2. *Let (P, M) be a rank one spot over (I, m). Then P is analytically unramified.*

Proof. By Corollary 4.1 P is a spot of type one, q. e. d.

Let (P, M) be a spot of type two over (I, m). The *every* set of t elements $y_1, \cdots, y_t$ in P which map modulo M onto a transcendence base for P/M over I/m are algebraically independent over I, hence the ring $B = I(y_1, \cdots, y_t)$ is a basic ring in P. (B is a rank two regular local ring, since the y_i are algebraically independent over I). Since P is a spot over I, $P = \mathfrak{o}_\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal in an affine ring $\mathfrak{o}$ over I. Since P/M is isomorphic to the quotient field of $\mathfrak{o}/\mathfrak{q}$, there exist $y_1, \cdots, y_t \in \mathfrak{o}$, $\notin \mathfrak{q}$ such that the y_i map modulo M onto a transcendence base for P/M over I/m.

Definition 4.3. *Let* $P = \mathfrak{o}_\mathfrak{q}$ *be a spot of type two over* (I, m). *A basic ring* B *in* P *is a special basic ring in* P *in case* $B = I(y_1, \cdots, y_t)$, *where* $y_1, \cdots, y_t$ *are elements in* $\mathfrak{o}$, *not in* $\mathfrak{q}$, *whose residues modulo* $\mathfrak{q}$ *are a transcendence base for* $\mathfrak{o}/\mathfrak{q}$ *over* I/m.

Remark 4.2. If P is a spot of type two over I, then P contains a special basic ring.

Remark 4.3. Every special basic ring in P is a rank two regular local ring.

LEMMA 4.4. *Let* $(P, M) = (\mathfrak{o}_\mathfrak{q}, \mathfrak{q}\mathfrak{o}_\mathfrak{q})$ *be a spot of type two over* (I, m), *let* $\operatorname{rank} P = r$, *and let* (B, mB) *be a special basic ring in* P, *where* $B = I(y_1, \cdots, y_t)$. *Then there exist* $r-2$ *elements in* $\mathfrak{q}$ *which are algebraically independent over* $A = I[y_1, \cdots, y_t]$.

Proof. Since P is a spot of type two, $r \geqq 2$ (Corollary 4.1). Since $\operatorname{rank} P = \operatorname{trd}(P/B) + 2$ (Corollary 3.4), $\operatorname{trd}(0/A) = r - 2$. If $r = 2$, then there is nothing to prove, so it may be assumed that $r > 2$. Hence there exists an element $z_1 \in \mathfrak{o}$ which is transcendental over A, and it may be assumed that $z_1 \notin \mathfrak{q}$. Then the residue z_1' of z_1 modulo $\mathfrak{q}$ is algebraic over $A/(\mathfrak{q} \cap A)$ (by the choice of the y_i). Let $f_1'(z_1') = 0$ be a (not necessarily monic) minimal equation of z_1' over $A/(\mathfrak{q} \cap A)$, and let $f_1(z_1) = x_1 \neq 0$ be an element in $\mathfrak{q}$ which maps modulo $\mathfrak{q}$ onto $f_1'(z_1')$. Since z_1 is transcendental over A, x_1 is transcendental over A. If $r = 3$, then the lemma is proved, so it may be assumed that $r > 3$. Then there exists an element $z_2 \in \mathfrak{o}$ such that z_2 is transcendental over $A[x_1]$, and it may be assumed that $z_2 \notin \mathfrak{q}$. As above let $f_2(z_2) = x_2$ be an element in $\mathfrak{q}$ which maps modulo $\mathfrak{q}$ onto a minimal equation $f_2'(z_2') = 0$ of z_2' over $A/(\mathfrak{q} \cap A)$. Then $x_2 \neq x_1$, $x_2 \neq 0$, and since z_2 is transcendental over $A[x_1]$, x_2 is transcendental over $A[x_1]$, hence x_1 and x_2 are algebraically independent over A. Hence in $r-2$ steps the required elements are obtained, q. e. d.

LEMMA 4.5. *Let (P, M) be a spot of type two over (I, m), and let* rank $P = r$ $(r \geqq 2)$. *Then there exists a special basic ring B^* in P and elements $z_1, \cdots, z_{r-2}$ in M which are algebraically independent over B^* such that P is a finite separable algebraic extension of $B^*[z_1, \cdots, z_{r-2}]$.*

Remark. The proof of this lemma is a direct generalization of Nagata's proof of Proposition 8 ([4], p. 397).

Proof. Since P is separably generated over I, when the characteristic of I is 0 the lemma is true by Lemma 4.4, so it may be assumed that the characteristic of I is $p \neq 0$. Let $P = \mathfrak{o}_{\mathfrak{q}}$, and let $B = I(y_1, \cdots, y_t)$ be a special basic ring in P (B exists by Remark 4.2). Let $A = I[y_1, \cdots, y_t]$, and let $x_1, \cdots, x_{r-2}$ be elements in $\mathfrak{q}$ which are algebraically independent over A (Lemma 4.4). Then $\operatorname{trd}(\mathfrak{o}/A[x_1, \cdots, x_{r-2}]) = 0$, hence $\operatorname{trd}(\mathfrak{o}/I) = t + (r-2)$. Let $n = t + r - 2$, let $w_i = x_i$ $(i = 1, \cdots, r-2)$, and let $w_{r-2+i} = y_i$ $(i = 1, \cdots, t)$. Since P is separably generated over I, let $D_1, \cdots, D_n$ be a maximal linearly independent set of derivations of $\mathfrak{o}$ over I (existence is proven in ([4], p. 390)). Let $u_1, \cdots, u_n$ be elements in $\mathfrak{o}$ such that $D_i u_j \neq 0$ if and only if $i = j$. It may be assumed that $u_j - 1 \in \mathfrak{q}$ $(j = 1, \cdots, n)$, since otherwise the elements $1 + u_j \alpha^p$ $(\alpha \in \mathfrak{q})$ are such that $D_i(1 + u_j \alpha^p) \neq 0$ if and only if $i = j$, and $(1 + u_j \alpha^p) - 1$ are in $\mathfrak{q}$. Set $z_j = w_j^p u_j$. Then $D_i z_j \neq 0$ if and only if $i = j$, hence $z_1, \cdots, z_n$ are a separating transcendence base for $\mathfrak{o}$ over I. Since $u_j - 1 \in \mathfrak{q}$, $z_j' = w_j'^p u_j' = w_j'^p$ (where the $'$ indicates residues modulo q). Now $w_j'^p = 0$ $(j = 1, \cdots, r-2)$, and the $w_j'^p$ $(j = r-1, \cdots, n)$ are a transcendence base for $\mathfrak{o}/\mathfrak{q}$ over I/m. Therefore the ring $B^* = I(z_{r-1}, \cdots, z_n)$ is a special basic ring in P, and the elements $z_1, \cdots, z_{r-2}$ are elements in $\mathfrak{q}$ which are algebraically independent over B^*, q. e. d.

PROPOSITION 4.3. *Let (P, M) be a spot over (I, m). If P is a spot of type two, then P is analytically unramified.*

Proof. Let rank $P = r$ $(r \geqq 2)$. Let (B, mB) be a special basic ring in P such that there exist elements $x_1, \cdots, x_{r-2}$ in M such that P is a finite separable algebraic extension of $C^* = B[x_1, \cdots, x_{r-2}]$ (Lemma 4.5). Set $Q^* = (mB, x_1, \cdots, x_{r-2})C^*$, $C = C^*_{Q^*}$, and $Q = Q^*C$. Since B is a regular local ring of rank two (Remark 4.3), and since the z_i are algebraically independent over B (Lemma 4.5), (C, Q) is a regular localy ring of rank r, and $P \geqq C$. Let E be the quotient field of C, and let L be the quotient field of P, so L is a finite separable algebraic extension of E. Hence, since C is a normal Noetherian domain, the integral closure C' of C in L is a finite

C-module ([9], pp. 264-265). Therefore the integral closure D of C in P is a finite C-module. Since P is a spot over B, there exists elements $d_1, \cdots, d_g \in P$ such that P is a quotient ring with respect to a prime ideal of the ring $C[d_1, \cdots, d_g]$, and since the d_i are algebraic over E, there exist elements $s_i \in C$ such that the elements $s_i d_i \in D$, hence the quotient field of D is L. Since $P \geqq D_{(M \cap D)} \geqq C$, $M \cap D$ is a maximal ideal in D and there exist elements $e_1, \cdots, e_k \in L$ such that P is a quotient ring with respect to a prime ideal of $D_{(M \cap D)}[e_1, \cdots, e_k]$. Hence by a recent result due to Rees [8], P is analytically unramified if $D_{(M \cap D)}$ is analytically unramified. Since D is a finite C-module, D is a semi-local domain, hence $D_{(M \cap D)}$ is analytically unramified if D is ([10], p. 283), and since C' is a semi-local domain which is a finite D-module, D is analytically unramified if C' is ([10], p. 277). Hence to prove that P is analytically unramified it is sufficient to prove that C' is analytically unramified.

Since L is a finite separable algebraic extension of E, let u be an element in C' such that $L = \sum_{i=0}^{\alpha} Eu^i$, and set $H = \sum_{i=0}^{\alpha} Cu^i$. Then H is an integral domain which contains C and is contained in C', hence H is a semi-local domain with quotient field L. Let F be the total quotient ring of the completion of H. Since C' is a finite C-module, there exists a nonzero element $d \in C$ such that $dC' \subseteq H$. Since the completion of C is a regular local ring ([10], p. 302), d is not a zero divisor in the completion of H ([10], p. 277), hence F contains the completion of C'. Let K be the quotient field of the completion of C. Then it is seen that $F = \sum_{i=0}^{\alpha} Ku^i$. Since F is a finite dimensional algebra over K which contains the completion of C' and is contained in the total quotient ring of the completion of C', F is the total quotient ring of the completion of C'. It is a straight forward verification that F is isomorphic to $L \otimes_E K$, and since L is separably generated over E, $L \otimes_E K$ contains no nonzero nilpotent elements ([9], p. 195). Therefore C' is analytically unramified, hence P is analytically unramified, q. e. d.

Propositions 4. 1, 4. 2, and 4. 3 constitute a proof of Theorem 4. 1.

It is known ([4], p. 414) that if a semi-local domain P is analytically unramified, then the derived normal ring of P is a finite P-module, hence

COROLLARY 4. 3. *If P is a spot which is separably generated over a ground ring I, then the derived normal ring of P is a finite P-module.*

As mentioned in the introduction, Nagata's proof that a Dedekind domain has the property (*SF*) is essentially based on statements 1. 1 and 1. 2. Since

Corollary 3.2 and Corollary 4.3 are respectively the generalizations of these statements to the case where I is a rank two regular local ring which has an infinite residue field, Nagata's proof carries over verbatim to prove

THEOREM 4.2. *If* $\mathfrak{o}$ *is an affine ring which is separably generated over a ground ring* I, *then the derived normal ring of* $\mathfrak{o}$ *is a finite* $\mathfrak{o}$*-module.*

UNIVERSITY OF IOWA.

REFERENCES.

[1] S. Abhyankar and O. Zariski, "Splitting of valuations in extensions of local domains," *Proceedings of the National Academy of Science, USA*, vol. 41 (1955), pp. 84-90.

[2] M. Nagata, "On the derived normal rings of Noetherian integral domains," *Memoirs of the College of Science, University of Kyoto*, Ser. A, vol. 29 (1955), pp. 293-303.

[3] ———, "A general theory of algebraic geometry over Dedekind domains, I," *American Journal of Mathematics*, vol. 78 (1956), pp. 78-116.

[4] ———, "A general theory of algebraic geometry over Dedekind domains, II," *American Journal of Mathematics*, vol. 80 (1958), pp. 382-420.

[5] ———, "On the chain problem of prime ideals," *Nagoya Mathematical Journal*, vol. 10 (1956), pp. 51-64.

[6] ———, "Note on a chain condition for prime ideals," *Memoirs of the College of Science, University of Kyoto*, Ser. A, vol. 32 (1959), pp. 85-90.

[7] D. G. Northcott, *Homological Algebra*, Cambridge University Press, 1960.

[8] D. Rees, "A note on analytically unramified local rings," *Journal of the London Mathematical Society*, vol. 36 (1961), pp. 24-28.

[9] O. Zariski and P. Samuel, *Commutative Algebra*, Volume I. D. van Nostrand Co., Inc., 1958.

[10] O. Zariski and P. Samuel, *Commutative Algebra*, Volume II. D. Van Nostrand Co., Inc., 1960.

UNIFORMLY BOUNDED REPRESENTATIONS, II.*

Analytic Continuation of the Principal Series of Representations of the $n \times n$ Complex Unimodular Group.

By R. A. KUNZE[1] and E. M. STEIN.[2]

0. Introduction. This paper is the second of a series devoted to the study of uniformly bounded representations of classical groups and the application of these representations to analysis on these groups.

In the previous paper [8], this was carried out for the special case of the 2×2 real unimodular group. Two related results were basic. The first dealt with the analytic continuation of the 'principal series' of representations —leading to a family of uniformly bounded representations defined in a strip. The second result applied the analytic family of representations to obtain a 'Hausdorff-Young Theorem' for the group together with its implications for the characterization of representations.

Our purpose here is to carry out the analytic continuation of the principal series in the case of the group of $n \times n$ complex unimodular matrices. The problems dealing with the continuation for other semi-simple groups and the problems connected with the Hausdorff-Young Theorem will be considered in future papers of this series.

We consider the group G of $n \times n$ complex unimodular matrices, and its diagonal (i.e., Cartan) sub-group C, whose entries we denote by $c = (c_1, c_2, \cdots, c_n)$, $c \in C$. Let λ denote a continuous character of the subgroup C. Then

$$(0.1) \qquad \lambda(c) = \left(\frac{c_1}{|c_1|}\right)^{m_1} \left(\frac{c_2}{|c_2|}\right)^{m_2} \cdots \left(\frac{c_n}{|c_n|}\right)^{m_n} \cdot |c_1|^{s_1} \cdots |c_n|^{s_n}$$

where $s_1, s_2, \cdots, s_n$ are complex numbers and $m_1, m_2, \cdots, m_n$ are integers; both sequences are uniquely determined if we require that $s_1 + s_2 + \cdots + s_n = 0$ and $0 \leqq m_1 + m_2 + \cdots + m_n < n$. (We call the integer r, $r = m_1 + m_2 + \cdots + m_n$, $0 \leqq r < n$, the *residue* of the character λ.) Notice that the character λ is unitary if $Re(s_j) = 0$, $j = 2, \cdots, n$.

---

* Received August 31, 1961.

[1] Research supported in part by National Science Foundation Grant No. 12847.

[2] Research supported in part by National Science Foundation Grant No. 14234.

Gelfand and Neumark have shown how to construct an irreducible unitary representation for each unitary character λ. This leads to the 'principal series' of representations; these are the representations which arise in the Plancherel formula for the group. They are constructed as follows.

For each such λ the representation $a \rightarrow T(a, \lambda)$ is realized as a multiplier representation on $L_2(V)$, where V is the sub-group of G consisting of matrices which have ones on the main diagonal and whose entries above the main diagonal vanish. The representation $T(a, \lambda)$ is defined by

$$T(a, \lambda) : f(v) \rightarrow K(va, \lambda) f(v\tilde{a}) \tag{0.2}$$

where K is an appropriate multiplier and the mapping $v \rightarrow v\tilde{a}$ may be thought of as a generalization of fractional linear transformations which occur when $n = 2$.

Now the multiplier appearing in (0.2) depends on λ and thus on $s_1, s_2, \cdots, s_n$. This dependence may in fact be seen to be analytic. Thus we can obtain in a trivial sense an analytic continuation of (0.2). This naive analytic continuation is, however, not the right one for a variety of reasons. The simplest of these is that the resulting operators are not uniformly bounded, in fact not everywhere defined on $L^2(V)$ when $Re(s_j) \neq 0$.*

The natural analytic continuation may be motivated by the following considerations.

We quote two known facts about the representations (0.2), (when $Re(s_j) = 0$). The first is that they already irreducible on a certain subgroup G_0 of G. The second fact is that $T(\cdot, \lambda)$ and $T(\cdot, p\lambda)$ are unitarily equivalent representations for any character λ and any permutation p of the character (i.e., element of the Weyl group of G).

It is convenient to group the characters λ into n distinct classes—(their residue classes). The class to which any character belongs is determined by the unique integer r, $0 \leqq r < n$, for which $m_1 + m_2 + m_3 + \cdots + m_n = r$. Or put another way, the class is determined by the action of λ on the center of G.

We come now to what is in effect a basic result of this paper. The representations $T(\cdot,\lambda_1)$ and $T(\cdot,\lambda_2)$ for which λ_1 and λ_2 belong to the same class are equivalent when restricted to G_0. This is remarkable in view of the fact that they are already irreducible on G_0. Thus there exists a unitary operator, $W(\lambda)$, so that if we define $R(a,\lambda)$ by

---

* It is possible to bypass the last objection and obtain by analytic continuation everywhere defined (but not uniformly bounded) representations by reformulating the representations (0.2) in terms of the maximal compact sub-group. See Harish-Chandra, "Representations of a semi-simple Lie group I," *Trans. Amer. Math. Soc.*, vol. 75 (1953), p. 241. It should be added, however, that in this sense there are infinitely many "analytic continuations" of the principal series. Only by adding certain natural considerations can one find a unique analytic continuation, which in addition, enjoys the further properties which are described hereafter.

$$R(a,\lambda) = W(\lambda)T(a,\lambda)W^{-1}(\lambda) \tag{0.3}$$

and if we fix $a \in G$, then $R(a,\lambda)$ depends only on the class of λ (and thus in particular is constant as a function of $s_1, s_2, \cdots, s_n$). In view of the already quoted irreducibility of $T(\cdot,\lambda)$ restricted to G_0, the representations $R(\cdot,\lambda)$ so determined are unique. We call these the ***normalized principal series.*** It is these representations that can be continued analytically in the parameters of λ while $T(a,\lambda)$ and $W(\lambda)$ separately can not.

The discussion above insures the existence of $W(\lambda)$ and thus $R(a,\lambda)$ *a priori*, but tells us nothing about their concrete properties which are necessary for analytic continuation. We need first, therefore, construct $W(\lambda)$ in explicit terms.

In order to get an idea of how to go about this, we recall, as mentioned above, that $T(\cdot,\lambda)$ and $T(\cdot,p\lambda)$ are unitarily equivalent; therefore $R(\cdot,\lambda)$ and $(R\cdot,p\lambda)$ are unitarily equivalent. Using the fact that $R(a,\lambda) = R(a,p\lambda)$ for $a \in G_0$, it follows (from the irreducibility on G_0) that $R(a,\lambda) = R(a,p\lambda)$ for all $a \in G$, and finally $W^{-1}(p\lambda)W(\lambda)T(a,\lambda) = T(a,p\lambda)W^{-1}(\lambda)W(p\lambda)$ for all p in the Weyl group.

This shows that an explicit determination of $W(\lambda)$ brings with it a similarly explicit description of the intertwining operators $A(p,\lambda)$ defined by $A(p,\lambda)T(a,\lambda) - T(a,p\lambda)A(p,\lambda)$.

We reverse the heuristic argument described above and begin our study by obtaining the intertwining operators $A(p,\lambda)$ in a concrete fashion. It turns out that this task is much simplified when we restrict ourselves to the $n-1$ permutations $p_1, p_2, \cdots, p_{n-1}$, where p_r corresponds to the transposition $(r, r+1)$ of the symmetric group on n letters. These $n-1$ permutations generate the whole Weyl group. It is then found that the operators $A(p_r,\lambda)$ can be given by singular convolution integrals whose kernels are carried on one-dimensional (complex) sub-groups of V (see Theorem 1, Section 4).

A basic property of the operators $A(p,\lambda)$ is that although they do not commute in general, they satisfy certain fundamental commutativity relations (see Theorem 2, Section 5). These commutativity relations are a reflection of the relations satisfied by the generators $p_1, p_2, \cdots, p_{n-1}$ of the Weyl group. The actual analysis of the commutativity relations is rather complex but is simplified by reducing the problem to the case of the 3×3 group by a change of variables. In this sense the 3×3 group is already the general case, because here we must deal with the non-commutativity of the sub-group $V(3)$, which makes the Fourier analysis on $L_2(V)$ difficult.

Once the properties of the operators $A(p, \lambda)$ are obtained, we can then define the operators $W(\lambda)$. These are given by products of $\frac{n(n-1)}{2}$ operators $A(p, \lambda)$, (see 6.5) and 5.17)). We then prove in Theorem 3 (Section 6) the basic properties of the normalized prinicipal series for unitary λ.

Our next task is the analytic continuation of this series. The problem of analytic continuation is tractable because of the following two considerations. 1) It suffices, in effect, to continue one parameter only keeping the others fixed. That this allows us to obtain analytic continuation simultaneously in all parameters follows from the lemmas of Section 8. 2) The group G is generated by the sub-group G_0 and a fixed element $p \in G$. Since the $R(a, \lambda)$, $a \in G_0$, have trivial (i.e., constant) analytic continuations, it suffices to consider the analytic continuation of the single operator $R(p, \lambda)$. Here use is made of the lemmas of Section 7.

The resulting uniformly bounded representations are defined when the parameters $s_1, s_2, \cdots, s_n$ vary over an open 'tube' in the complex hyperplane $s_1 + s_2 + \cdots + s_n = 0$. Their basic properties are set forth in Theorem 4 of Section 9.

In Section 10 we calculate the 'trace' of these representations which allows us to prove in particular the following: (i) $R(\cdot, \lambda)$ is unitary if and only if $\lambda' = p(\lambda)$, where λ' is the complex contragredient character of λ, and p is some element of the Weyl group. Hence $R(\cdot, \lambda)$ is unitary if and only if it corresponds to an element of the principal or complementary series. (ii) If $\lambda' \neq p(\lambda)$, then although $R(\cdot, \lambda)$ is uniformly bounded, it is not equivalent to a unitary representation.

1. The principal series.

In this section we recall relevant facts about G and the construction of the principal series. Detailed proofs of most of the results we state below may be found in the book by Gelfand and Neumark [3].[8]

Let $GL = GL(n)$ denote the group of all complex non-singular matrices of degree n. In what follows we shall need to consider the following subgroups of GL.

---

[8] In stating the results of Gelfand and Neumark we have found it convenient to use a notation which is different from theirs.

$G = G(n)$: the unimodular sub-group.

$C = C(n)$: the (Cartan) sub-group of diagonal matrices $c = [c_1, c_2, \cdots, c_n]$ in G.

$U = U(n)$: the upper triangular unipotent matrices

$$u = \begin{bmatrix} 1 & u_{12} & \cdots & u_{1n} \\ \cdot & \cdot\cdot & \cdot\cdot\cdot & \cdot\cdot \\ 0 & \cdot\cdot & \cdot\cdot\cdot & 1 \end{bmatrix}.$$

$u_{jk} = 0$ for $j > k$ and $u_{jj} = 1$.

$V = V(n)$: the lower triangular unipotent matrices

$$v = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \cdot\cdot & \cdot\cdot\cdot & \cdot\cdot & \cdot \\ v_{n1} & \cdots & v_{nn-1} & 1 \end{bmatrix}$$

$v_{jk} = 0$ for $j < k$ and $v_{jj} = 1$.

For each a in GL, let

$$\begin{pmatrix} j_1 & \cdots & j_m \\ k_1 & \cdots & k_m \end{pmatrix}$$

be the determinant of the submatrix of a formed from rows $j_1, \cdots, j_m$ and columns $k_1, \cdots, k_m$ of a. Put

$$(1.1) \qquad D_j(a) = \begin{pmatrix} j & j+1 & \cdots & n \\ j & j+1 & \cdots & n \end{pmatrix}$$

$$D_{n+1}(a) = 1.$$

Then in order that a may be expressed as a product

$$(1.2) \qquad a = ucv, \ u \in U, \ v \in V, \ c \text{ diagonal}$$

it is necessary and sufficient that $D_j(a) \neq 0$ for $1 \leqq j \leqq n$. The matrices u, v, and c are then uniquely determined as follows: Let

$$(1.3) \qquad D_{jk}(a) = \begin{pmatrix} j & j+1 & \cdots & n \\ j & k+1 & \cdots & n \end{pmatrix}, \ j < k$$

$$(1.4) \qquad D_{jk}(a) = \begin{pmatrix} j & j+1 & \cdots & n \\ j & k+1 & \cdots & n \end{pmatrix}, \ j > k.$$

Then u, v, and c are given by

$$u_{jk} = \frac{D_{jk}(a)}{D_k(a)}, \quad j < k \tag{1.5}$$

$$v_{jk} = \frac{D_{jk}(a)}{D_j(a)}, \quad j > k \tag{1.6}$$

$$c_j = \frac{D_a(a)}{D_{j+1}(a)}, \quad 1 \leqq j \leqq n. \tag{1.7}$$

If $a \in GL$ and all the determinants $D_j(a)$ are different from 0, we shall say that a is *decomposable.* The diagonal matrix c in (1.2) will be called the diagonal part of a and will be denoted by $\operatorname{diag}(a)$. It should be noted that $\operatorname{diag}(a)$ belongs to C, i. e., has determinant 1 if and only if a is in G.

The elements v of V are parametrized by the real and imaginary parts, x_{jk}, y_{jk} of their entries v_{jk}. The measure dv obtained by taking the product of the differentials

$$dv_{jk} = dx_{jk}dy_{jk}, \quad j > k \tag{1.8}$$

is both left and right invariant; so V is unimodular.

In the 2×2 case, V may be identified with the additive group of complex numbers, and GL then acts on V as the group of linear fractional transformations. In the general case GL acts on V in a similar fashion. We shall now describe this action. Let a be a fixed member of GL. Then for v in V, the determinants $D_j(va)$ are polynomial functions of the entries v_{jk} of v. Thus, with the exception of a lower dimensional set of measure 0, the product va is decomposable; the exceptional set of elements v depends on a. If va can be expressed as a product $u'c'v'$ with $u' \in U$, $v' \in V$, and c' diagonal, then this can be done in only one way and we shall put

$$v\tilde{a} = v'. \tag{1.9}$$

In the 2×2 case, $v\tilde{a}$ is the element of V defined by

$$(v\tilde{a})_{21} = \frac{v_{21}a_{11} + a_{21}}{v_{21}a_{12} + a_{22}}. \tag{1.10}$$

When n is arbitrary, there are still some instances in which $v\tilde{a}$ is easily described. For example, if c is diagonal, $v\tilde{c} = c^{-1}vc$, and for any $v_1 \in V$, $v\tilde{v}_1 = vv_1$.

Let $v \in V$, $a \in GL$, and suppose va is decomposable. If b is any member of GL, then vab is decomposable if and only if $(v\tilde{a})b$ is; when this is the case it is then true that

$$v(\widetilde{ab}) = (v\tilde{a})\tilde{b}. \tag{1.11}$$

When $n=2$, the mapping $v \rightarrow v\tilde{a}$ induces a transformation of the real parameters corresponding to v_{21} whose Jacobian is equal to

$$|\det a|^2 \cdot |v_{21}a_{12}+a_{22}|^{-4}.$$

Thus the measure $d(v\tilde{a})$ is given by

$$d(v\tilde{a}) = |\det a|^2 \cdot |v_{21}a_{12}+a_{22}|^{-4}\, dv. \tag{1.12}$$

In the general case, the measure $d(v\tilde{a})$ is obtained as follows: Let μ be the character of the diagonal sub-group of GL given by

$$\mu(c) = \prod_{j=1}^{n} |c_j|^{2(n-2j+1)}. \tag{1.13}$$

For each decomposable a in GL, let

$$\mu(a) = \mu(c)$$

where c is the diagonal part of a in the decomposition (1.2). Then with a fixed, $\mu(va)$ as a function of v is defined on all but a set of measure 0 in V; and

$$d(v\tilde{a}) = \mu(va)\, dv. \tag{1.14}$$

This is proved in [3] for the case in which a has determinpant 1. The general case may be deduced from this with the aid of the following observations. (i) If $a \in GL$ and b is a non-zero scalar multiple of a then a and b determine the same transformation of V; furthermore, (1.6) and (1.7) show that the digaonal parts of va and vb differ by a multiplicative factor. (ii) if $a \in GL$ then $(\det a)^{-1/n} a \in G$. (iii) In (1.13) the sum of the exponents is equal to 0.

If λ is any character of the diagonal sub-group of GL its domain of definition may be extended as above. Thus if $a = ucv$ with $u \in U$, $v \in V$, and c diagonal we shall put

$$\lambda(a) = \lambda(c). \tag{1.15}$$

After this extension λ is no longer multiplicative but has the following properties. If c is diagonal and a is decomposable, then ca and ac are decomposable, and

$$\lambda(ca) = \lambda(ac) = \lambda(c)\lambda(a). \tag{1.16}$$

If $v \in V$ then $\lambda(v) = 1$, and

$$\lambda(vab) = \lambda(va)\lambda[(v\tilde{a})b] \tag{1.17}$$

whenever va and vab are both decomposable.

We shall say that a character of C is *unitary* if it maps C into the multiplicative group of complex numbers of absolute value 1. To each continuous unitary character λ of C is associated a unitary representation $a \to T(a, \lambda)$ of G on the Hilbert space, $L_2(V)$ of square integrable functions on V. These representations are known as the *principal series* and are defined for f in $L_2(V)$ by

$$T(a, \lambda) f(v) = \lambda(va) \mu^{\frac{1}{2}}(va) f(v\tilde{a}). \tag{1.18}$$

2. The decomposition $V = ZZ'$. In this section we decompose V into the product of two sub-groups Z and Z' and study the action of G on V in terms of this decomposition.

Let l and m be integers such that $1 \leqq l < m \leqq n$ and $m - l < n - 1$. For each $a \in G$, let $\dot{a}$ be the $n \times n$ matrix specified by the following conditions.

(i) $\dot{a}_{jk} = a_{jk}$, $l \leqq j, k \leqq m$.

(ii) $\dot{a}_{kk} = 1$, $k < l$ or $k > m$.

(iii) $\dot{a}_{jk} = 0$ in the cases not covered by (i) or (ii).

We shall denote by $\hat{a}$ the submatrix of a formed from the entries a_{jk}, $l \leqq j$, $k \leqq m$. The mapping $v \to \dot{v}$, $v \in V$ is a homomorphism of V onto a subgroup $Z = Z(l, m)$; Z is contained in V and is isomorphic to $V(m - l + 1)$ via the mapping $z \to \hat{z}$. Let $Z' = Z(l, m)'$ be the kernel of the homomorphism $v \to \dot{v}$. The $n \times n$ identity matrix is the only element of V which is common to both Z and to Z'. Moreover, an easy computation shows that $\dot{v}^{-1} v \in Z'$ for each v in V. Thus to each $v \in V$ there correspond unique elements z and z' such that

$$v = zz', \quad z \in Z, \quad z' \in Z'. \tag{2.1}$$

To illustrate we consider the case $n = 4$. A typical element of $Z(2, 4)$ has the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & v_{32} & 1 & 0 \\ 0 & v_{42} & v_{43} & 1 \end{bmatrix}$$

whereas a typical element of $Z(2, 3)'$ has the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ v_{21} & 1 & 0 & 0 \\ v_{31} & 0 & 1 & 0 \\ v_{41} & v_{42} & v_{43} & 1 \end{bmatrix}.$$

We shall denote by dz the invariant measure in Z obtained from the product of the differentials (1.8)

$$dz_{jk} = dx_{jk}dy_{jk} \qquad l \leqq k < j \leqq m.$$

Since Z' is a closed normal sub-group of V, it follows ([9; p. 133]) that Z' is unimodular and also ([9; p. 119]) that

$$dv = dz\, dz' \tag{2.2}$$

where dz' is a suitably chosen invariant measure on Z'. We shall not need the explicit form of dz' (actually, here the most obvious candidate for dz' works).

If $b = \dot{a}$ is non-singular, the mapping $z \to z\tilde{b}$ is well defined and carries Z into Z. The transformed measure $d(z\tilde{b})$ is obtained as follows: Let $\mu_{l,m}$ be thet character of C defined by

$$\mu_{l,m} = \prod_{j=l}^{m} | c_j |^{2(m+1-2j)}. \tag{2.3}$$

It then follows from (1.13) and (1.14) applied to the case $n = m - l + 1$ that

$$d(z\tilde{b}) = \mu_{l,m}(ab)\, dz. \tag{2.4}$$

For certain a in G, $b = \dot{a}$ is non-singular, and the mapping $z \to z\tilde{a}$, $z \in Z$ coincides with the mapping $z \to z\tilde{b}$. We shall be interested in two sub-groups of G whose elements have this property. One of the sub-groups is the diagonal sub-group C. For suppose $c \in C$. Then $z\tilde{c} = \dot{c}^{-1}zc$ for each z in Z, and since

$$(c^{-1}zc)_{jk} = c_j^{-1}z_{jk}c_k$$

it is evident that c and $\dot{c}$ induce the same mapping of Z into Z. The other sub-group we shall call $U^+ = U^+(l, m)$. It contains U and is obtained as follows: Let $X = X(l, m)$ be the sub-group of G consisting of all x such that $x = \dot{x}$. The mapping $x \to \hat{x}$, $x \in X$ is an isomorphism between X and $G(m - l + 1)$. In addition, denote by $Y = Y(l, m)$ the kernel of the homomorphism $u = \dot{u}$, $u \in U$. It is then easily seen that $X \cap Y = \{1_n\}$, that X is in the normalizer of Y in G, and that the product, XY is a sub-group of G. We shall put $U^+ = XY$. To illustrate we again consider the case $n = 4$. A typical element of $U^+(2, 3)$ has the form

$$\begin{bmatrix} 1 & U_{12} & U_{13} & U_{14} \\ 0 & U_{22} & U_{23} & U_{24} \\ 0 & U_{32} & U_{33} & U_{34} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let us now determine in general how an element of U^+ acts on Z. To do this we ask when an element xy of U^+ is decomposable. Since $xyx^{-1} \in U$ and $xy = xyx^{-1} \cdot x$ it follows that xy is decomposable if and only if x is decomposable; furthermore, the elements c and v in the decomposition (1.2) of xy depend only on x. On the other hand, since X is isomorphic to $G(m-l+1)$ it is evident that c and v are members of X and in fact that $v \in Z$. From these observations we obtain the following result.

LEMMA 1. *Let $z \in Z$, $x \in X$, and $y \in Y$. Then zxy is decomposable if and only if zx is decomposable. If zx and zxy are decomposable then*

$$z\widetilde{xy} = z\tilde{x} \in Z \tag{1}$$

$$\operatorname{diag}(zxy) = \operatorname{diag}(zx) \in X. \tag{2}$$

3. The operators $A(p, \lambda)$. In this section we shall use the decompositions $V = ZZ'$ in defining a class of operators $A(p, \lambda)$ in $L_2(V)$. These operators play a crucial role in our work on the representations of G. In order to understand something about their group theoretic significance it will be necessary to introduce some terminology.

Let k be an integer such that $1 \leqq k \leqq n-1$, and $Z = Z(k, k+1)$. Let $p = p_k$ be the element of $X = X(k, k+1)$ which satisfies

$$\hat{p} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{3.1}$$[4]

Suppose in addition that $m_1, m_2, \cdots, m_n$ are integers, that $s_1, s_2, \cdots, s_n$ are complex numbers, and that λ is the character of C given by

$$\lambda(c) = \prod_{j=1}^{n} \left(\frac{c_j}{|c_j|} \right)^{m_j} |c_j|^{s_j}. \tag{3.2}$$

We shall now obtain an explicit expression for the function $\lambda(zp)$, $z \in Z$. If $z \in Z$ then

$$\hat{z} = \begin{bmatrix} 1 & 0 \\ z_{k+1k} & 1 \end{bmatrix}.$$

Hence the mapping $z \rightarrow z_{k+1k}$ is an isomorphism between Z and the additive group of complex numbers; to simplify the notation we shall also denote z_{k+1k} by z. We use this convention in the statement of the following lemma.

---

[4] For further clarification of the role of the matrices p_k see the discussion at the beginning of Section 4 and in Section 6 following equation (6.4).

LEMMA 2. *Suppose $z \in Z$, $u \in U$, and that λ is defined by* (3.2). *Then for $z \neq 0$,*

$$\lambda(zup) = \lambda(zp) = \left(\frac{z}{|z|}\right)^{m_{k+1}-m_k} |z|^{s_{k+1}-s_k}.$$

Proof. Since $U^+ = XY$ we may write $u = xy$, $x \in X$, $y \in Y$ (actually $x = \dot{u}$). Thus $zup = zxyp = zxp(p^{-1}yp)$. Because Y is normal in U^+, $p^{-1}yp \in Y$, and it follows from Lemma 1 that zup is decomposable if and only if zxp is decomposable.

In addition we have

$$\hat{x} = \hat{u} = \begin{bmatrix} 1 & u_{kk+1} \\ 0 & 1 \end{bmatrix}.$$

Now if we also write x for u_{kk+1} it follows that

$$\hat{z}\hat{x}\hat{p} = \begin{bmatrix} 1 & 0 \\ z & 1 \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -x & 1 \\ -zx-1 & z \end{bmatrix}.$$

Hence if $z \neq 0$,

$$zxp = \begin{bmatrix} 1 & \frac{1}{z} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{z} & 0 \\ 0 & z \end{bmatrix}\begin{bmatrix} 1 & 0 \\ \frac{zx+1}{-z} & 1 \end{bmatrix}.$$

From this we see that zup and zp are decomposable if and only if $z = z_{k+1k} \neq 0$; if this is so, $\operatorname{diag}(zup) = \operatorname{diag}(zp) = c \in X$,

$$\hat{c} = \begin{bmatrix} \frac{1}{z} & 0 \\ z & 0 \end{bmatrix}$$

and by (1.15)

$$\lambda(zup) = \lambda(zp) = \lambda(c) = \left(\frac{z}{|z|}\right)^{m_{k+1}-m_k} |z|^{s_{k+1}-s_k}.$$

Now let μ be the character of C defined by (1.13). Applying Lemma 2 we obtain

$$\gamma(m,s) = i^{|m|}\pi 2^s \left(\frac{z}{|z|}\right)^{m_k-m_{k+1}} |z|^{-2+s_k-s_{k+1}}. \tag{3.5}$$

The operators $A(p,\lambda)$ are defined in $L_2(V)$ at least formally by the integral

$$A(p,\lambda)f(v) = \frac{1}{\gamma(\lambda)}\int_Z \lambda^{-1}(zp)\mu^{\frac{1}{2}}(zp)f(z^{-1}v)\,dz. \tag{3.4}$$

The factor $\gamma(\lambda) = \gamma(m_k - m_{k+1}, s_k - s_{k+1})$, where for any integer m and complex number s

$$(3.5) \qquad \gamma(m,s) = i^{|m|}\pi 2^s \frac{\Gamma\left(\frac{|m|+s}{2}\right)}{\Gamma\left(\frac{|m|+2-s}{2}\right)}.$$

To study the operators $A(p,\lambda)$ we introduce another class of operators. If m is an integer and s is a complex number, $0 < Re(s) < 1$, we define an operator $A(p,m,s)$ in $L_2(V)$ by

$$(3.6) \qquad A(p,m,s)f(v) = \frac{1}{\gamma(m,s)} \int \left(\frac{z}{|z|}\right)^m |z|^{-2+s} f(z^{-1}v)\,dz.$$

As we shall show, the integral in (3.6) is well defined and $A(p,m,s)f \in L_2(V)$ for a dense set of functions f in $L_2(V)$. Thus (3.4) will define an operator in $L_2(V)$ whenever $0 < Re(s_k - s_{k+1}) < 1$. For the domain D of the operators $A(p,m,s)$ we shall take all bounded Baire functions with compact support.

LEMMA 3. *Let m be an integer, s a complex number, $0 < Re(s) < 1$, and f an element of D. Then*

(1) *(3.6) converges absolutely for all $v \in V$;*

(2) *$A(p,m,s)f \in L_2(V)$;*

(3) *the mapping $s \to A(p,m,s)f$ has a unique extension to $Re(s) = 0$, so that as a function of s with values in $L_2(V)$ it is continuous in $0 \leqq Re(s) < 1$;*

(4) *if $Re(s) = 0$, the operators $A(p,m,s)$ are isometric and extend (uniquely) to unitary operators on $L_2(V)$;*

(5) *if $Re(s_1) = Re(s_2) = 0$ then*

$$A(p,m_1,s_1)A(p,m_2,s_2) = A(p,m_1+m_2,s_1+s_2)$$

for all integers m_1 and m_2;

(6) *$A(p,0,0) = I =$ the identity.*

Proof. (1) If f is a function on V, it follows from (2.1) that we may write $f(v) = f(zz') = f(z,z')$. In addition, if f is integrable (2.2) shows that

$$\int f(v)\,dv = \int\int f(z,z')\,dz\,dz'.$$

Thus if we identitfy z with its entry z_{k+1k} and use the fact that Z is isomorphic to the additive group of complex numbers, we may rewrite (3.6) as

$$(3.7) \qquad A(p,m,s)f(z,z') = \frac{1}{\gamma(m,s)} \int \left(\frac{w}{|w|}\right)^m |w|^{-2+s} f(z-w,z')\,dw.$$

In this integral w is a single complex variable, and dw is the 2-dimensional element of area. If we take absolute values in (3.7) and disregard the multiplicative constant, we have

$$|A(p,m,s)f(z,z')| \leqq \int |w|^{-2+s_0} |f(z+w,z')| \, dw$$

where $s_0 = Re(s)$, $0 < s_0 < 1$. Therefore

$$|A(p,m,s)f(z,z')|$$
$$\leqq \int_{|w| \leqq 1} |w|^{-2+s_0} |f(z+w,z')| \, dw + \int_{|w|>1} |w|^{-2+s_0} |f(z+w,z')| \, dw.$$

We shall denote the first integral by $g_1(z,z')$ and the second by $g_2(z,z')$. Since $0 < s_0 < 1$, $|w|^{-2+s_0}$ is integrable over the unit disc and square integrable over the set where $|w| > 1$. Because $|f(w,z')|$ is bounded and has compact support as a function of w, it therefore follows that the integrals defining g_1, g_2 exist for all z, z'. This proves (1).

(2) Let K be a compact set containing the support of $f(z,z')$, K_1 the projection of K on Z, and K_2 the projection of K on Z'. Then K_1, K_2 are both compact and have finite measures $|K_1|$, $|K_2|$. Denoting lub $|f|$ by M and using Young's inequality, we obtain

$$\int |g_1(z,z')|^2 \, dz \leqq |K_1| \Big(\int_{|w| \leqq 1} |w|^{-2+s_0} dw \Big)^2 < \infty$$

and

$$\int |g_2(z,z')|^2 \, dz \leqq M^2 |K_1|^2 \cdot \int_{|w|>1} |w|^{-4+s_0} dw < \infty.$$

If $g(z,z') = A(p,m,s)f(z,z')$, it follows that

$$\int |g(z,z')|^2 \, dz \leqq \text{Constant} \cdot M^2 (|K_1| + |K_2|^2).$$

Note that $f(z,z') = 0$ if $z' \notin K_2$. Hence $g(z,z') = 0$ when $z' \notin K_2$. Therefore

$$\int \int |g(z,z')|^2 \, dz dz' \leqq \text{Constant} \cdot M^2 (|K_1| + |K_1|^2) |K_2| < \infty$$

which proves (2).

(3) Let t be a complex variable. Then the Fourier transform of $f(z,z')$ with respect to the z variable is the function $\hat{f}(t,z')$ given by

$$\hat{f}(t,z') = \frac{1}{2\pi} \int e^{-i\, Re(t\bar{z})} f(z,z') \, dz. \tag{3.8}$$

Let us put $\hat{H}_\epsilon(w) = \dfrac{1}{\gamma(m,s)} e^{-\epsilon|w|} \Big(\dfrac{w}{|w|} \Big)^m |w|^{-2+s}$, $\epsilon \geqq 0$. We need the following fact (see Bochner [1], p. 39). If $t \neq 0$

$$\lim_{\epsilon \downarrow 0} \int \hat{H}_\epsilon(w) e^{-i\,Re(t\bar{w})} dw = \left(\frac{t}{|t|}\right)^m |t|^{-s}.$$

We shall also put $g_\epsilon(z, z') = \int H_\epsilon(w) f(z - w, z') dw$ for $\epsilon \geqq 0$. Then $A(p, m, s) f(z, z') = g_0(z, z')$, and the argument used in (1) and (2) shows that g_ϵ, $\epsilon > 0$, also belongs to $L_2(V)$. Applying the dominated convergence theorem, we see that $g_\epsilon(z, z') \to g_0(z, z')$ for each z, z'. For $\epsilon \geqq 0$, g_ϵ is dominated by the $L_2(V)$ function

$$h(z, z') = \int \frac{|w|^{-2+s_0}}{|\gamma(m, s)|} |f(z - w, z')|\, dw.$$

A second application of domianted convergence shows that $g_\epsilon \to g_0$ in $L_2(V)$. We now denote by $\hat{g}_\epsilon(t, z')$ the Fourier transform (3.8) of $g_\epsilon(z, z')$, $\epsilon \geqq 0$. By the Plancherel theorem, we see that $\hat{g}_\epsilon(t, z') \to \hat{g}_0(t, z')$ in the $L_2(t, z')$ norm. On the other hand,

$$\hat{g}_\epsilon(t, z') = 2\pi \cdot H_\epsilon(t) \hat{f}(t, z'), \ \epsilon > 0.$$

Since $2\pi \cdot H_\epsilon(t) \to \left(\frac{t}{|t|}\right)^m |t|^{-s}$, $t \neq 0$, we find that

$$(A(p, m, s) f)^\wedge = \hat{g}_0(t, z') = \left(\frac{t}{|t|}\right)^m |t|^{-s} \hat{f}(t, z'). \tag{3.9}$$

It follows from the Plancherel theorem that we may use (3.9) to extend the definition of $A(p, m, s) f$ to all s in the strip $0 \leqq Re(s) < 1$. To prove the continuity of $A(p, m, s) f$ as a function of s with values in $L_2(V)$ it is then sufficient to show that

$$\int\int \left| \left(\frac{t}{|t|}\right)^m \hat{f}(t, z') \right|^2 \left| |t|^{-s} - |t|^{-s_1} \right|^2 dt\, dz' \to 0$$

as $s \to s_1$, $0 \leqq Re(s) < 1$, $0 \leqq Re(s_1) < 1$. We recall that f is bounded and vanishes outside the compact set K; hence, $\hat{f}(t, z')$ is bounded and vanishes when $z' \notin K_2$. Thus the above expression is bounded by

$$\text{Constant} \cdot \int_{K_2} \int_{|t| \leqq 1} \left| |t|^{-s} - |t|^{-s_1} \right|^2 dt\, dz'$$
$$+ \int_{K_2} \int_{|t| \leqq 1} \left| |t|^{-s} - |t|^{-s_1} \right|^2 |\hat{f}(t, z')|^2 dt\, dz'.$$

An easy application of the Lebesgue dominated convergence theorem shows that both integrals tend to 0 as $s \to s_1$.

It is obvious that the mapping $s \to A(p, m, s) f$ has at most one continuous extension to the strip $0 \leqq Re(s) < 1$, and the proofs of (4), (5) and (6) follows immediately from (3.9) and Plancherel's theorem. This concludes the proof of Lemma 3.

4. The intertwining properties of the operators $A(p, \lambda)$. Let S be the sub-group of G which is generated by the unitary matrices $p = p_k$, $1 \leqq k \leqq n-1$. Then S is contained in the normalizer of C, and there is little difficulty in showing that S is finite. For the purposes of this paper it will be convenient to refer to S as the Weyl group.[5]

If λ is a character of C and $q \in S$, the mapping $c \to \lambda(q^{-1}cp)$, $c \in C$ is again a character. We denote this character by $q\lambda$. Let us now suppose $a \to T(a, \lambda)$ and $a \to T(a, \lambda_1)$ are two members of the principal series. Then by a fundamental theorem of Gelfand and Neumark [3] these representations are unitarily equivalent if and only if there is an element q of S such that $\lambda_1 = q\lambda$.

Their proof of this result is in part abstract, and in part quite concrete; however, it yields only the existence of the intertwining operators.[6] In this section we shall exhibit specific intertwining operators between the representations $a \to T(a, \lambda)$ and $a \to T(a, p\lambda)$, $p = p_k$, $1 \leqq k \leqq n-1$.

Let λ be the character of C defined by

$$\lambda(c) = \prod_{j=1}^{m} \left(\frac{c_j}{|c_j|} \right)^{m_j} |c_j|^{s_j} \tag{4.1}$$

where $m_1, m_2, \cdots, m_n$ are integers and $s_1, s_2, \cdots, s_n$ are complex numbers such that $0 \leqq Re(s_j) < \frac{1}{2}$, $1 \leqq j \leqq n$. If $p = p_k$, $1 \leqq k \leqq n-1$ we shall put

$$A(p, \lambda) = A(p, m_k - m_{k+1}, s_k - s_{k+1})$$

It follows from Lemma 2 and (3.4) that $A(p, \lambda)$ is independent of the representation of λ given by (4.1). One can also see this directly. For if we also have

$$\lambda(c) \prod_{j=1}^{n} \left(\frac{c_j}{|c_j|} \right)^{m'_j} |c_j|^{s'_j}$$

where $m'_1, m'_2, \cdots, m'_n$ are integers and $s'_1, s'_2, \cdots, s'_n$ are complex numbers then there is an integer l and a complex number w such that $m_j = m'_j + l$ and $s_j = s'_j + w$, $1 \leqq j \leqq n$. Hence

$$m_j - m_{j+1} = m'_j - m'_{j+1} \text{ and } s_j - s_{j+1} = s'_j - s'_{j+1}, \qquad 1 \leqq j \leqq n.$$

---

[5] The Weyl group as it is usually defined may be identified with a quotient group of S.

[6] In recent note (Doklady 1960, vol. 131, pp. 496-499; also Soviet Mathematics 1960, vol. 1, no. 2, pp. 276-279) Gelfand and Graev have announced some results dealing with integrals of the type (3.4).

When $Re(s_k - s_{k+1}) = 0$, $A(p,\lambda)$ is unitary on $L_2(V)$ (Lemma 3) and otherwise $A(p,\lambda)$ is unbounded—with domain D consisting of all bounded Baire functions vanishing outside compact subsets of V.

We recall that every continuous unitary character of C has the form (4.1) where $s_1, s_2, \cdots, s_n$ are purely imaginary, i.e., $Re(s_j) = 0$, $1 \leqq j \leqq n$.

THEOREM 1. *Let G be the $n \times n$ complex unimodular group, λ a continuous unitary character of the diagonal sub-group, and $a \to T(a,\lambda)$ the corresponding member of the principal series. Then if $p = p_k$, $1 \leqq k \leqq n-1$.*

$$A(p,\lambda)T(a,\lambda) = T(a,p\lambda)A(p,\lambda) \tag{4.2}$$

for all $a \in G$.

Roughly speaking, the main idea of the proof is to first establish (4.2) for a class of non-unitary characters. The necessity for this arises from the fact that the operators $A(p,\lambda)$ are not given explicitly by (3.4) when λ is unitary. The result is then obtained for unitary characters by a limiting argument. In the proof we shall need a series of lemmas.

If $p = p_k$, $1 \leqq k \leqq n-1$, let μ_p be the character of C defined by

$$\mu_p(c) = |c_k|^2 \, |c_{k+1}|^{-2}. \tag{4.3}$$

LEMMA 4. *Let $1 \leqq k \leqq n-1$, $p = p_k$, and $Z = Z(k, k+1)$. Suppose $z \in Z$, and $a = cu$, $c \in C$, $u \in U$. Then*

(1) $d(z\tilde{a}) = \mu_p(za)\,dz$;

(2) $\mu_p(zu) = \mu(zu)$;

(3) $\mu_p(c) = \mu^{\frac{1}{2}}(c)\mu^{\frac{1}{2}}(p^{-1}cp)$.

Proof. (1) By definition, μ_p is the character μ_{kk+1} given by (2.3). Thus if $b = \dot{a}$, it follows from (2.4) that $d(z\tilde{b}) = \mu_p(zb)\,dz$. On the other hand, since $b = \dot{c}\dot{u}$, $z\tilde{a} = (z\tilde{c})\tilde{u} = z\tilde{b}$, $z \in Z$. Hence, $d(z\tilde{a}) = \mu_p(zb)\,dz$. We also have $\mu_p(za) = \mu_p(cc^{-1}zcu) = \mu_p(c)\mu_p(c^{-1}zcu)$. By (4.3), $\mu_p(c) = \mu_p(\dot{c})$, and Lemma 1 shows that $\mu_p(c^{-1}zcu) = \mu_p(c^{-1}zc\dot{u})$. Thus

$$\mu_p(za) = \mu_p(\dot{c})\mu_p(c^{-1}zc\dot{u}) = \mu_p(ab).$$

(2) Suppose zu is decomposable. Then by Lemma 1, $\operatorname{diag}(zu) = c$ belongs to $X(k, k+1)$. Hence $c_k c_{k+1} = 1$, and from (1.13) we find that $\mu(c) = |c_k|^{2(n-2k+1)} \, |c_{k+1}|^{2(n-2k-1)} = |c_k|^2 \, |c_{k+1}|^{-2} = \mu_p(c)$. Thus $\mu(zu) = \mu(c) = \mu_p(c) = \mu_p(zu)$.

(3) It is easily verified that $(p^{-1}cp)_k = c_{k+1}$, $(p^{-1}cp)_{k+1} = c_k$, and $(p^{-1}cp)_j = c_j$ for $j \neq k$ and $j \neq k+1$. Thus

$$\begin{aligned}\mu^{\frac{1}{2}}(c)\mu^{-\frac{1}{2}}(p^{-1}cp) &= |\,c_k\,|^{n-2k+1}\,|\,c_{k+1}\,|^{n-2k-1}\,|\,c_{k+1}\,|^{2k-n-1}\,|\,c_k\,|^{2k-n+1}\\ &= |\,c_k\,|^{2}\,|\,c_{k+1}\,|^{-2}\\ &= \mu_p(c).\end{aligned}$$

This establishes (3) and concludes the proof of Lemma 4.

Let a be a decomposable element of G and λ a continuous character of C. In order to simplify the notation we shall set

$$K(a,\lambda) = \lambda(a)\mu^{\frac{1}{2}}(a). \tag{4.4}$$

If a is not decomposable, we put $K(a,\lambda) = 0$. It follows that

$$K(va,\lambda) = \lambda(va)\mu^{\frac{1}{2}}(va),\ v \in V,\ a \in G \tag{4.5}$$

and that

$$K(zp,\lambda^{-1}) = \lambda^{-1}(zp)\mu^{\frac{1}{2}}(zp),\ z \in Z. \tag{4.6}$$

We recall that D is the collection of all bounded Baire functions vanishing outside compact subsets of V. For f in D, let

$$T(a,\lambda)f(v) = K(va,\lambda)f(v\tilde{a}). \tag{4.7}$$

It will also be convenient to denote the character contragredient to a given character λ and λ'. Thus

$$\lambda'(c) = \bar{\lambda}(c^{-1}),\ c \in C. \tag{4.8}$$

In the next three lemmas we suppose the following:

(i) $p = p_k,\ 1 \leqq k \leqq n-1$.
(ii) $a \in G,\ f \in D$, and $g \in D$.
(iii) λ is given by (4.1) and $0 < Re(s_k - s_{k+1}) < 1$.
(iv) $\lambda_1 = (p\lambda)'$.

In addition, we shall denote the inner product

$$\int f_1(v)\overline{f_2(v)}\,dv$$

of two functions f_1, f_2 in $L_2(V)$ by (f_1, f_2).

LEMMA 5. *Suppose $T(a,\lambda)f \in L_2(V)$. Then the integral*

$$\int_Z K(zva,\lambda)K(z^{-1}p,\lambda^{-1})f[(zv)\tilde{a}]\,dz$$

exists for almost all v in V, $A(p,\lambda)g \in L_2(V)$, and

$$(T(a,\lambda)f, A(p,\bar{\lambda})g)$$
$$= \frac{1}{\gamma(\lambda)} \int_V \overline{g(v)}\, dv \int_Z K(zva,\lambda) K(z^{-1}p,\lambda^{-1}) f[(zv)\tilde{a}]\, dz.$$

Proof. By Lemma 3, $A(p,\bar{\lambda})g \in L_2(V)$, and an easy computation shows that

$$\frac{K(z^{-1}p,\lambda^{-1})}{\gamma(\lambda)} = \frac{K(zp,\lambda')}{\gamma(\bar{\lambda})} . \tag{4.9}$$

Thus

$$(T(a,\lambda)f, A(p,\bar{\lambda})g)$$
$$= \frac{1}{\gamma(\lambda)} \int_V K(va,\lambda) f(v\tilde{a})\, dv \int_Z K(z^{-1}p,\lambda^{-1}) \bar{g}(z^{-1}v)\, dz.$$

Now, $K(va,\lambda)f(v\tilde{a})K(z^{-1}p,\lambda^{-1})\bar{g}(z^{-1}v)$ is a Baire function on $V \times Z$ and

$$\int_V | K(va,\lambda) f(v\tilde{a}) |\, dv \int_Z | K(z^{-1}p,\lambda^{-1}) \bar{g}(z^{-1}v) |\, dz < \infty. \tag{4.10}$$

Thus, by Fubini's theorem

$$(T(a,\lambda)f, A(p,\bar{\lambda})g) = \iint_{V\times Z} K(va,\lambda) K(z^{-1}p,\lambda^{-1}) f(v\tilde{a}) \bar{g}(z^{-1}v)\, dx dz.$$

Since the homeomorphism $(v,z) \to (zv,z)$ is measure preserving,

$$(T(a,\lambda)f, A(p,\bar{\lambda})g) = \iint_{V\times Z} K(zva,\lambda) K(z^{-1}p,\lambda^{-1}) f[(zv)\tilde{a}] \bar{g}(v)\, dv dz.$$

The stated result now follows from a second application of Fubini's theorem.

LEMMA 6. *Suppose* $T(a^{-1},\lambda_1)g \in L_2(V)$. *Then the integral*

$$\int_Z K(va,p\lambda) K(z^{-1}p,\lambda^{-1}) f[z(v\tilde{a})]\, dz$$

exists for almost all v *in* V, *and*

$$(A(p,\lambda)f, T(a^{-1},\lambda_1)g) = \int_V \bar{g}(v)\, dv \int_Z K(va,p\lambda) K(z^{-1}p,\lambda^{-1}) f[z(v\tilde{a})]\, dz.$$

Proof. By Lemma 3, $A(p,\lambda)f \in L_2(V)$. Thus

$$(A(p,\lambda)f, T(a^{-1},\lambda_1)g)$$
$$= \frac{1}{\gamma(\lambda)} \int A(p,\lambda)f(v) K(va^{-1},\bar{\lambda}_1) \bar{g}(v\tilde{a}^{-1})\, dv.$$

On the other hand, since $d(v\tilde{a}) = \mu(va)\,dv$,

$$(A(p,\lambda)f, T(a^{-1},\lambda_1)g) = \frac{1}{\gamma(\lambda)}\int A(p,\lambda)f(v\tilde{a})K[(v\tilde{a})a^{-1},\bar{\lambda}_1]\bar{g}(v)\mu(va)\,dv.$$

By (1.17), $K[(v\tilde{a}^{-1},\bar{\lambda}_1] = \lambda_1'(va)\mu^{-\frac{1}{2}}(va)$, and as $\lambda_1' = p\lambda$ we find that

$$\begin{aligned}(A(p,\ )f, T(a^{-1},\lambda_1)g) \\ &= \frac{1}{\gamma(\lambda)}\int A(p,\lambda)f(v\tilde{a})K(va,p\lambda)\bar{g}(v)\,dv \\ &= \frac{1}{\gamma(\lambda)}\int_V \bar{g}(v)\,dv \int_Z K(va,p\lambda)K(z^{-1}p,\lambda^{-1})f[z(v\tilde{a})]\,dz.\end{aligned}$$

LEMMA 7. *Suppose both $T(a,\lambda)f$ and $T(a^{-1},\lambda_1)g$ belong to $L_2(V)$. Then*

$$(T(a,\lambda)f, A(p,\bar{\lambda})g) = (A(p,\lambda)f, T(a^{-1},\lambda_1)g).$$

Proof. It is easily verified that

$$K(z^{-1}p,\lambda^{-1}) = (-1)^{m_k-m_{k+1}}K(zp,\lambda^{-1}). \tag{4.11}$$

By Lemmas 5 and 6, it is therefore sufficient to show that for almost all v

$$\int_Z K(zva,\lambda)K(ap,\lambda)f[(zv)\tilde{a}]\,dz = \int_Z K(va,p\lambda)K(zp,\lambda^{-1})f[z(v\tilde{a})]\,dz. \tag{4.12}$$

In order to do this, we first observe that corresponding to a, there is a measurable subset V_a of V such that (i) $V - V_a$ has measure 0, (ii) the integrals in (4.12) exist for $v \in V_a$, and (iii) va is decomposable for each $v \in V_a$. To each $v \in V_a$ there is a corresponding element $b = uc$ in UC such that $va = b(v\tilde{a})$. In addition, there is a measurable subset $Z_{v,a}$ of Z, depending on v and a, with the property that $Z - Z_{v,a}$ has measure 0 and ab is decomposable for each $z \in Z_{v,a}$. Since the mapping $z \to z\tilde{b}$ carries Z into Z and $d(z\tilde{b}) = \mu_p(zb)\,dz$ (Lemma 4), it follows that the second integral in (4.2) is equal to

$$\int_{Z_{v,a}} K(va,p\lambda)K[(z\tilde{b})p,\lambda^{-1}]f[(a\tilde{b})(v\tilde{a})]\mu_p(zb)\,dz. \tag{4.13}$$

If z is a fixed element of $Z_{v,a}$ there are matrices u_1 and c_1 in U and C respectively such that $zu = u_1c_1(z\tilde{u})$. Since $b = uc$, $zb = zuc = u_1c_1c \cdot c^{-1}(zu)c = u_1c_1c(z\tilde{b})$. Thus $\operatorname{diag}(zb) = c_1c$ and $zva = zb(v\tilde{a}) = u_1 \cdot c_1c \cdot (z\tilde{b})(v\tilde{a})$. It follows that zva is decomposable, that $\operatorname{diag}(zva) = c_1c$, and that $(zv)\tilde{a} = (z\tilde{b})(v\tilde{a})$. Hence upon comparing (4.13) with the first integral in (4.12) we see that it is sufficient to prove

$$K(zp,\lambda^{-1})K(c_1c,\lambda) = K(c,p\lambda)\mu_p(c_1c)K[(z\tilde{b})p,\lambda^{-1}]. \tag{4.14}$$

Now from the definition (4.4) of K and the multiplicative properties (1.16), (1.17) of the functions λ, μ it follows that

$$\begin{aligned} K[(z\tilde{b})p,\lambda^{-1}] &= K[c^{-1}(z\tilde{u})cp,\lambda^{-1}] \\ &= K(c^{-1},\lambda^{-1})K[(z\tilde{u})p\cdot p^{-1}cp,\lambda^{-1}] \\ &= K(c^{-1},\lambda^{-1})K(p^{-1}cp,\lambda^{-1})K[(z\tilde{u})p,\lambda^{-1}]. \end{aligned}$$

By Lemma 1, $K(zp,\lambda^{-1}) = K(zup,\lambda^{-1})$, and on the other hand,

$$\begin{aligned} K(zup,\lambda^{-1}) &= K(zu,\lambda^{-1})K[(z\tilde{u})p,\lambda^{-1}] \\ &= K(c_1,\lambda^{-1})K[(z\tilde{u})p,\lambda^{-1}]. \end{aligned}$$

From this we obtain the relation

$$K[(z\tilde{b})p,\lambda^{-1}] = K(c^{-1},\lambda^{-1})K(p^{-1}cp,\lambda^{-1})K(c_1^{-1},\lambda^{-1})K(zp,\lambda^{-1}).$$

Therefore (4.14) reduces to the condition

$$\begin{aligned} &K(c_1,\lambda)K(c_1,\lambda^{-1})\mu_p(c_1^{-1}) \\ &\quad = K(c^{-1},\lambda)K(c,p\lambda)\mu_p(c)K(c^{-1},\lambda^{-1})K(p^{-1}cp,\lambda^{-1}). \end{aligned} \tag{4.15}$$

The left side of (4.15) equals $\mu(c_1)\mu_p(c_1^{-1})$, and this equals 1 by part (2) of Lemma 4.

In the right side of (4.15), the product $K(c,p\lambda)K(p^{-1}cp,\lambda^{-1}) = \mu^{\frac{1}{2}}(c)\mu^{\frac{1}{2}}(p^{-1}cp)$, while $K(c^{-1},\lambda)K(c^{-1},\lambda^{-1}) = \mu^{\frac{1}{2}}(c^{-1})\mu^{\frac{1}{2}}(c^{-1})$. Thus the right side of (4.15) reduces to $\mu_p(c)\mu^{-\frac{1}{2}}(c)\mu^{\frac{1}{2}}(p^{-1}cp)$, and this equals 1 by part (3) of Lemma 4. This finishes the proof of (4.12).

LEMMA 8. *Let λ be a continuous unitary character of C and $p = p_k$, $1 \leqq k \leqq n-1$. For $0 < s < \frac{1}{2}$ and $c \in C$, let $\lambda^{(s)}(c) = |c_k|^s\lambda(c)$, and $\lambda_1^{(s)}(c) = |c_{k+1}|^{-s}\lambda(p^{-1}cp)$. Then, corresponding to each a in G, there exist subsets $D(a,\lambda)$ and $D(a^{-1},p\lambda)$ of D with the following properties.*

(1) *$D(a,\lambda)$ and $D(a^{-1},p\lambda)$ are dense in $L_2(V)$.*

(2) *For f in $D(a,\lambda)$*

$$\lim_{s\downarrow 0}\|T(a,\lambda)f - T(a,\lambda^{(s)})f\|_2 = 0.$$

(3) *For g in $D(a^{-1},p\lambda)$*

$$\lim_{s\downarrow 0}\|T(a^{-1},p\lambda)g - T(a^{-1},\lambda^{(s)})g\|_2 = 0.$$

Proof. Let $f \in D$. Then by (1.7) and the definition of $T(a,\lambda^{(s)})f$, it follows that

$$\begin{aligned} T(a,\lambda^{(s)})f(v) &= [h(v)]^s T(a,\lambda)f(v) \\ &= [h(v)]^s\mu(va)\mu^{\frac{1}{2}}(va)f(v\bar{a}) \end{aligned}$$

where $h(v) = \left| \dfrac{D_k(va)}{D_{k+1}(va)} \right|$. We also have

$$T(a^{-1}, \lambda_1^{(s)})f(v) = [h_1(v)]^s T(a^{-1}, p\lambda)f(v)$$

where $h_1(v) = \left| \dfrac{D_{k+2}(va)}{D_{k+1}(va)} \right|$.

Let E be the collection of all functions f in $L_2(V)$ with the property that $h^{\frac{1}{2}} \cdot T(a, \lambda)f$ belongs to $L_2(V)$. Since h is measurable and $T(a, \lambda)$ is unitary, E is dense in $L_2(V)$. If f is in D and $\epsilon > 0$, standard measure theoretic arguments show the existence of a function f_ϵ in D such that $\| f - f_\epsilon \|_2 < \epsilon$ and $| f_\epsilon(v) | \leqq | f(v) |$ a.e.. Hence $| T(a, \lambda) f_\epsilon(v) | \leqq | T(a, \lambda) f(v) |$ a.e., and therefore f_ϵ belongs to E. Let $D(a, \lambda) = D \cap E$. What we have just done shows $D(a, \lambda)$ is dense in $L_2(V)$.

If $f \in D(a, \lambda)$ and $0 < s < \frac{1}{2}$ then

$$| h(v) |^s \, | T(a, \lambda) f(v) | \leqq (h^{\frac{1}{2}}(v) + 1) \, | T(a, \lambda) f(v) | \tag{4.16}$$

for all v in V. In addition,

$$T(a, \lambda) f(v) = \lim_{s \downarrow 0} | h(v) |^s \, T(a, \lambda) f(v).$$

Since the right side of (4.16) is a function in $L_2(V)$, it follows from the Lebesgue dominated convergence theorem that

$$\lim_{s \downarrow 0} \| T(a, \lambda) f - T(a, \lambda^{(s)}) f \|_2 = 0.$$

Now let $D(a^{-1}, p\lambda)$ be the collection of all functions f in D such that $h_1^{\frac{1}{2}} \cdot T(a^{-1}, p\lambda) f$ belongs to $L_2(V)$. Then the validity of (3) and the fact that $D(a^{-1}, p\lambda)$ is dense in $L_2(V)$ are seen by exactly the same arguments as we have used above.

Proof of Theorem 1. We suppose $p = p_k$, $1 \leqq k \leqq n - 1$, and that λ is a continuous unitary character of C. Let $\lambda^{(s)}$, $\lambda_1^{(s)}$, $D(a, \lambda)$, and $D(a^{-1}, p\lambda)$ be defined as in Lemma 8. Then in order to verify (4.2), it is sufficient to show that

$$(A(p, \lambda) T(a, \lambda) f, g) = (T(a, p\lambda) A(p, \lambda) f, g)$$

for $f \in D(a, \lambda)$ and $g \in D(a^{-1}, p\lambda)$. Now (5) and (6) of Lemma 3 tell us that the adjoint, $A(p, \lambda)^*$, of $A(p, \lambda)$ equals $A(p, \bar{\lambda})$. On the other hand, the adjoint of the unitary operator $T(a, p\lambda)$ equals $T(a^{-1}, p\lambda)$. Thus, to prove the theorem, we need only show that

$$(T(a, \lambda) f, A(p, \bar{\lambda}) g) = (A(p, \lambda) f, T(a^{-1}, p\lambda) g) \tag{4.17}$$

for $f \in D(a, \lambda)$ and $g \in D(a^{-1}, p\lambda)$. Let $0 < s < \frac{1}{2}$, $f \in D(a, \lambda)$, and $g \in D(a^{-1}, p\lambda)$. Then both $T(a, \lambda^{(s)})f$ and $T(a^{-1}, \lambda_1^{(s)})g$ belong to $L_2(V)$. In addition, $\lambda_1^{(s)} = [p \cdot \lambda^{(s)}]$, i.e., $\lambda_1^{(s)}$ is the contragradient of $p \cdot \lambda^{(s)}$. It follows from Lemma 7 that

$$(4.18) \qquad (T(a, \lambda^{(s)})f, A(p, \lambda^{(s)})g) = (A(p, \overline{\lambda^{(s)}})f, T(a^{-1}, \lambda_1^{(s)})g).$$

As s tends to 0 through positive values, the left and right sides of (4.18) tend to the left and right sides respectively of (4.17) (Lemma 3 and Lemma 8). This concludes the proof of Theorem 1.

5. Commutation relations satisfied by the operators $A(p, \lambda)$. Let $p = p_k$ and $q = p_j$, $1 \leqq j, k \leqq n-1$. Then by (4.2), $A(q, \lambda)T(a, \lambda) = T(a, q\lambda)A(q, \lambda)$ for all unitary characters λ. It follows that

$$\begin{aligned} A(p, q\lambda)A(q, \lambda)T(a, \lambda) &= A(p, q\lambda)T(a, q\lambda)A(q, \lambda) \\ &= T(a, pq\lambda)A(p, q\lambda)A(q, \lambda). \end{aligned}$$

Here we have used the fact that $(pq)\lambda = p(q\lambda)$. Thus $A(p, q\lambda)A(q, \lambda)$ is an intertwining operator for the representations, $a \to T(a, \lambda)$ and $a \to T(a, pq\lambda)$. Let us now suppose that $1 \leqq k \leqq n-2$ and that $q = p_{k+1}$, $p = p_k$. It is easy to see that $pqp = qpq$. Thus we can write down two intertwining operators for the representations corresponding to λ and $pqp\lambda$, namely

$$A(p, pq\lambda)A(q, p\lambda)A(p, \lambda)$$

and $A(q, pq\lambda)A(p, q\lambda)A(q, \lambda)$. We shall show that these apparently distinct operators are in fact identical. That they differ by at most a scalar factor of absolute value 1 is clear from the fact [3] that the representations of the principal series are irreducible. Our proof will not use irreducibility. We present it because it brings to light additional properties of the operators that will be used later on.

The operator $A(p, \lambda)$ equals $A(p, m_k - m_{k+1}, s_k - s_{k+1})$ where λ is given by (4.1) and $Re(s_j) = 0$, $1 \leqq j \leqq n$. From the definition of q, it follows that $A(p, q\lambda) = A(p, m_k - m_{k+2}, s_k - s_{k+2})$. Similarly,

$$A(q, \lambda) = A(q, m_{k+1} - m_{k+2}, s_{k+1} - s_{k+2}) \text{ and}$$
$$A(q, p\lambda) = A(q, m_k - m_{k+2}, s_k - s_{k+2}).$$

We also have

$$A(p, qp\lambda) = A(p, m_{k+1} - m_{k+2}, s_{k+1} - s_{k+2}), \text{ and}$$
$$A(q, pq\lambda) = A(q, m_k - m_{k+1}, s_k - s_{k+1}).$$

Using these relations we see that the equality of the above intertwining operators for all λ is equivalent to the validity of

$$\begin{aligned} &A(p, m_1, s_1)A(q, m_1+m_2, s_1+s_2)A(p, m_2, s_2) \\ &\qquad = A(q, m_2, s_2)A(p, m_1+m_2, s_1+s_2)A(q, m_1, s_1) \end{aligned} \tag{5.1}$$

for all integers m_1, m_2 and all complex numbers s_1, s_2—subject to the conditions, $Re(s_1) = 0$, $Re(s_2) = 0$. If we replace m_1, s_1 by $-m_1$, $-s_1$ and use (5) of Lemma 3 we find that (5.1) is equivalent to

$$\begin{aligned} &A(p, -m_1, -s_1)A(q, -m_1, -s_1)A(q, m_2, s_2)A(p, m_2, s_2) \\ &\qquad = A(q, m_2, s_2)A(p, m_2, s_2)A(p, -m_1, -s_1)A(q, -m_1, -s_1). \end{aligned} \tag{5.2}$$

By (5) and (6) of Lemma 3

$$A(p, -m_1, -s_1)A(q, -m_1, -s_1) = [A(q, m_1, s_1)A(p, m_1, s_1)]^{-1}.$$

Thus (5.2) is equivalent to the statement that the unitary operators $A(q, m, s)A(p, m, s)$, $Re(s) = 0$ form a commutative family;[7] however, the operators $A(q, m, s)$ and $A(p, m, s)$ do not commute (when $p = p_k$, $q = p_{k+1}$).

THEOREM 2. *Let* $p = p_k$ *and* $q = p_j$, $1 \leqq k < j \leqq n-1$. *Then the operators* $A(q, m, s)A(p, m, s)$, $Re(s) = 0$, m *an integer, form a commutative family of unitary operators on* $L_2(V)$, *and* $A(q, m, s)$ *commutes with* $A(p, m, s)$ *for all* m, s *if and only if* $j - k > 1$.

Proof. Suppose $j - k > 1$. Then it is easily seen that the matrices in $Z(k, k+1)$ commute with those in $Z(j, j+1)$ (see Section 2). From this observation and (3.6) it follows by a simple argument that $A(p, m, s)$ commutes with $A(q, m, s)$.

We suppose now that $j = k+1$ and consider the decomposition $V = ZZ'$ where $Z = Z(k, k+2)$. Then Z is isomorphic to $V(3)$ and contains the subgroups $Z(k, k+1)$ and $Z(k+1, k+2)$. In addition $dv = dzdz'$, and if f is a function on V, we may write $f(v) = f(zz') = f(z, z')$. If f is a bounded Baire function with compact support on V, and $0 < Re(s) < 1$, it therefore follows from (3.6) that

$$A(q, m, s)f(z, z') = \frac{1}{\gamma(m, s)} \int \left(\frac{z_k}{|z_k|}\right)^m |z_k|^{-2+s} f(z_k^{-1}z, z')\,dz_k \tag{5.3a}$$

and

$$A(p, m, s)f(z, z') = \frac{1}{\gamma(m, s)} \int \left(\frac{z_{k+1}}{|z_{k+1}|}\right)^m |z_{k+1}|^{-2+s} f(z_{k+1}^{-1}z, z')\,dz_{k+1}. \tag{5.3b}$$

---

[7] The various equivalent forms of (5.1) were pointed out to us by W. F. Stinespring.

In (5.3a) and (5.3b) the integration is extended over the sub-groups $Z(k, k+1)$ and $Z(k+1, k+2)$ respectively. Thus neither of our operators affects the second variable z', and it is therefore sufficient to prove the remainder of the theorem in the case $n=3$. Thus in what follows we shall consider the group $V(3)$ consisting of all complex matrices of the form

$$v = \begin{bmatrix} 1 & 0 & 0 \\ v_{21} & 1 & 0 \\ v_{21} & v_{32} & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ v_1 & 1 & 0 \\ v_3 & v_2 & 1 \end{bmatrix}.$$

We shall sometimes denote an element v of $V(3)$ by (v_1, v_2, v_3). If $w = (w_1, w_2, w_3)$ then

$$(5.4) \qquad wv = (w_1 + v_1, w_2 + v_2, w_3 + v_3 + w_2 v_1)$$

and $w^{-1} = (-w_1, -w_2, w_1 w_2 - w_3)$. The sub-groups $Z(1,2)$ and $Z(2,3)$ are given as follows: $Z(1,2)$ consists of all elements of the form $z_1 = (z_1, 0, 0)$ while $Z(2,3)$ is the set of all elements of the form $(0, z_2, 0)$. Rewriting (5.3a) and (5.3b) with the aid of (5.4) we obtain

$$(5.5a) \qquad A(p,m,s)f(v) = \frac{1}{\gamma(m,s)} \int \left(\frac{z_1}{|z_1|}\right)^m |z_1|^{-2+s} f(z_1^{-1} v)\, dz_1$$
$$= \frac{1}{\gamma(m,s)} \int \left(\frac{z}{|z|}\right)^m |z|^{-2+s} f(v_1 - z, v_2, v_3)\, dz$$

and

$$(5.5b) \qquad A(q,m,s)f(v) = \frac{1}{\gamma(m,s)} \int \left(\frac{z_2}{|z_2|}\right)^m |z_2|^{-2+s} f(z_2^{-1} v)\, dz_2$$
$$= \frac{1}{\gamma(m,s)} \int \left(\frac{z}{|z|}\right)^m |z|^{-2+s} f(v_1, v_2 - z, v_3 - z v_1)\, dz.$$

When $Re(s) = 0$, $A(p,m,s)$ and $A(q,m,s)$ are defined as in Lemma 3.

To analyze the products $A(q,m,s)A(p,m,s)$, $Re(s) = 0$, it will be convenient to introduce another unitary operator E, which is closely related to the Fourier-Plancherel transform on $V(3)$—studied by Godement in [4]. In defining E we first denote by E_1, the unitary operator characterized by the condition

$$(5.6) \qquad E_1 f(v_1, v_2, v_3 = f(v_1 - \frac{\bar{v}_2}{\bar{v}_3}, v_2, v_3), \quad v_3 \neq 0.$$

It follows easily from the classical Plancherel theorem that there is a unique unitary E_2 on $L_2(V)$ such that

$$(5.7) \qquad E_2f(v_1, v_2, v_3) = \frac{1}{(2\pi)^2} \int e^{-iRe(v_2\bar{w}_2+v_3\bar{w}_3)} f(v_1, w_2, w_3)\, dw_2 dw_3$$

whenever $f \in L_2(V)$ and $f(v_1, w_2, w_3)$ is integrable with respect to w_2, w_3. We now put $E = E_1E_2$.

LEMMA 9. *Let $Re(s) = 0$ and $f \in L_2(V)$. Then*

$$(5.8) \qquad EA(q, m, s) f(v_1, v_2, v_3) = \left(\frac{v_3\bar{v}_1}{|v_3\bar{v}_1|}\right)^m |v_3v_1|^{-s} Ef(v_1, v_2, v_3).$$

Proof. Consider first the case in which $0 < Re(s) < 1$ and f is a bounded function with compact support. Then by Lemma 3, $A(q, m, s) f \in L_2(V)$. Let us put

$$H_\epsilon(z) = \frac{e^{-\epsilon|z|}}{\gamma(m, s)} \left(\frac{z}{|z|}\right)^m |z|^{-2+s}, \quad \epsilon \geqq 0$$

and

$$g_\epsilon(v_1, v_2, v_3) = \int H_\epsilon(z) f(v_1, v_2 - z, v_3 - zv_1)\, dz.$$

Then $g_0 = A(p, m, s) f$, and $g_\epsilon \to g_0$ in $L_2(V)$ as $\epsilon \to 0$. The argument showing this is similar to one given in the proof of Lemma 3. If $\epsilon > 0$ we have

$$\begin{aligned} \int\int |g_\epsilon(v_1, v_2, v_3)|\, dv_2 dv_3 & \\ &\leqq \int dv_2 dv_3 \int |H_\epsilon(z)|\, |f(v_1, v_2 - z, v_3 - zv_1|\, dz \\ &= \int |H_\epsilon(z)|\, dz \int |f(v_1, v_2 - z, v_3 - zv_1)|\, dv_2 dv_3 \\ &= \int |H_\epsilon(z)|\, dz \cdot \int |f({}_1, v_2, v_3)|\, dv_2 dv_3 \\ &< +\infty. \end{aligned}$$

Hence we may use (5.7) to compute E_2g_ϵ. Interchanging the order of integration and changing variables in the resulting triple integral, we find that

$$E_2g_\epsilon(v) = \hat{f}(v_1, v_2, v_3) \int H_\epsilon(z) e^{-iRe[(v_2+v_3\bar{v}_1)\bar{z}]} dz.$$

Thus by (5.6)

$$Eg_\epsilon(v) = Ef(v) \int H_\epsilon(z) e^{-iRe(v_3\bar{v}_1\bar{z})} dz.$$

As $\epsilon \to 0$, $\| EA(q, m, s) f - Eg_\epsilon \|_2 \to 0$ and

$$\int H_\epsilon(z) e^{-iRe(v_3\bar{v}_1\bar{z})} dz \to \left(\frac{v_3\bar{v}_1}{|v_2\bar{v}_1|}\right)^m |v_3\bar{v}_1|^{-s}, \quad v_3\bar{v}_1 \neq 0.$$

It should be noted that (5.8) holds for all f in $L_2(V)$ whenever $Re(s) = 0$. It follows that

$$EA(q,m,s)f(v_1,v_2,v_3) = \left(\frac{v_3\bar{v}_1}{|v_3\bar{v}_1|}\right)^m |v_3v_1|^{-s}Ef(v_1,v_2,v_3).$$

We now let $s \to s_0$ where $Re(s_0) = 0$. Since E is bounded, Lemma 3 shows that $EA(q,m,s)f \to EA(q,m,s_0)f$ in $L_2(V)$. On the other hand, the right side of the above equation tends to $\left(\frac{v_3\bar{v}_1}{|v_3\bar{v}_1|}\right)^m |v_3v_1|^{-s_0}Ef(v_1,v_2,v_3)$, both pointwise and in the norm. This proves (5.8) when f is bounded and has compact support. The validity of (5.8), for all functions in $L_2(V)$, now follows by routine arguments.

LEMMA 10. *If $Re(s) = 0$, $A(p,m,s)$ commutes with E.*

Proof. Let $f(v_1,v_2,v_3) = g(v_1)h(v_2,v_3)$ where g and h are bounded and have compact supports. Then from (5.5a) and Lemma 3 we see that $A(p,m,s)f = (A(m,s)g)h$, $0 \leqq Re(s) < 1$, where $A(m,s)$ is the operator $A(p,m,s)$ in the case $n = 2$; thus we have

$$A(m,s)g(v_1) = \frac{1}{\gamma(m,s)}\int\left(\frac{z}{|z|}\right)^m |z|^{-2+s}g(v_1 - z)dz, \quad 0 < Re(s) < 1. \tag{5.9}$$

It now follows easily from (5.7) and (5.6) that $EA(p,m,s)f = A(p,m,s)Ef$, $0 \leqq Re(s) < 1$. Since $A(p,m,s)$ is bounded, for $Re(s) = 0$ and finite sums of functions of the form gh are dense in $L_2(V)$, it follows that $A(p,m,s)$ commutes with E whenever $Re(s) = 0$.

We have already defined the operators $A(m,s)$ on $L_2(v_1)$. It will be convenient at this point to introduce another family of operators $B(m,s)$. These are defined on $L_2(v_1)$, when m is an integer and $Re(s) = 0$, by

$$B(m,s)f(v_1) = \left(\frac{v_1}{|v_1|}\right)^{-m} |v_1|^{-s}f(v_1). \tag{5.10}$$

It should be noted that $B(0,0)$ is the identity operator and that

$$B(m_1,s_1)B(m_2,s_2) = B(m_1+m_2, s_1+s_2).$$

Now let $Re(s) = 0$ and suppose $f \in L_2(V)$. Then upon replacing f by $E^{-1}A(p,m,s)f$ in (5.8) and using Lemma 10, we obtain the relation

$$\begin{aligned} &EA(q,m,s)A(p,m,s)E^{-1}f(v_1,v_2,v_3) \\ &\quad = \left(\frac{v_3}{|v_3|}\right)^m |v_3|^{-s}\left(\frac{v_1}{|v_1|}\right)^{-m} |v|^{-s}A(p,m,s)f(v_1,v_2,v_3). \end{aligned} \tag{5.11}$$

In (5.11) we next set $f = gh$ where $g \in L_2(v_1)$ and $h \in L_2(v_2, v_3)$. Rewriting the right side of (5.11), with the aid of (5.10), we find that

$$\begin{aligned} &EA(q,m,s)A(p,m,s)E^{-1}f(v_1,v_2,v_3) \\ (5.12) \qquad &= \left(\frac{v_3}{|v_3|}\right)^m |v_3|^{-s}(B(m,s)A(m,s)g(v_1))h(v_2,v_3). \end{aligned}$$

Thus the operators $A(q,m,s)A(p,m,s)$ form a commutative family if and only if the operators $B(m,s)A(m,s)$ do. We shall finish the proof of Theorem 2 by showing that this is indeed the case. We should also remark that $B(m,s)$ does not commute with $A(m,s)$ if $m \neq 0$ or $s \neq 0$.

Lemma 11. *Let $V = V(2)$. Then the unitary operators $B(m,s)A(m,s)$ on $L_2(V)$, m an integer, and $Re(s) = 0$, form a commutative family.*

Proof. For each complex number $z \neq 0$, let L_z be the operator defined on Baire functions f by

$$L_z f(v) = f(z^{-1}v), \quad v \in V.$$

Then $L_z^{-1} = L_{z^{-1}}$ and since $\int |f(v)|^2 dv = |z|^{-2} \int |f(z^{-1}v)|^2 dv$, L_z is bounded on $L_2(dv)$; on the other hand, L_z is easily seen to be unitary on the space $L_2(|v|^{-2}dv)$. A straightforward computation shows that

$$(5.13) \qquad L_z B(m,s) L_z^{-1} = \left(\frac{z}{|z|}\right)^m |z|^s B(m,s).$$

Next consider $A(m,s)f$ where $0 < Re(s) < 1$ and f is a bounded function with compact support. A simple argument by change of variables shows

$$L_z A(m,s) L_z^{-1} f = \left(\frac{z}{|z|}\right)^{-m} |z|^{-s} A(m,s)f.$$

Using statement (3) of Lemma 3, we then obtain the relation

$$(5.15) \qquad L_z A(m,s) L_z^{-1} = \left(\frac{z}{|z|}\right)^{-m} |z|^{-s} A(m,s), Re(s) = 0.$$

Combining (5.13) and (5.15) we find that

$$(5.16) \qquad L_z B(m,s) A(m,s) = B(m,s) A(m,s) L_z, \quad z \neq 0.$$

In order to finish the proof, it will suffice, in view of (5.16), to show that the operators L_z, $z \neq 0$ generate a maximal abelian (self-adjoint) algebra of bounded operators on $L_2(dv)$. We shall prove this with the aid of the isometric mapping, M of $L_2(dv)$ onto $L_2(|v|^{-2}dv)$ which takes $f(v)$ into $vf(v)$. If $z \neq 0$, we have $L_z M f(v) = Mf(z^{-1}v) = z^{-1}vf(z^{-1}v) = z^{-1}ML_z f(v)$. Thus

$L_zM = z^{-1}ML_z$ or $ML_zM^{-1} = zL_z$. Hence the weakly closed algebra generated by the operators ML_zM^{-1} on $L_2(|v|^{-2}dv)$ coincides with the algebra generated by the unitary operators L_z; since $|v|^{-2}dv$ is a Haar measure on the multiplicative group of complex numbers, it follows, by a well known result, that the translations L_z generate a maximal abelian algebra on $L_2(|v|^{-2}dv)$.

This concludes the proof of the lemma and the proof of Theorem 2 as well.

COROLLARY. *If m is an integer and $Re(s) = 0$, let $J(k, m, s)$, $1 \leqq k \leqq n-1$, be the unitary operator on $L_2(V)$ given by*

$$(5.17) \qquad J(k, m, s) = A(p_{n-1}, m, s) \cdots A(p_{k+1}, m, s) A(p_k, m, s).$$

Then for fixed k, the operators $J(k, m, s)$ obtained by varying m and s form a commutative family.

Proof. Since $J(n-1, m, s) = A(p_{n-1}, m, s)$, the corollary in this case follows from Lemma 3. If $n > 2$, $J(n-2, m, s) = A(p_{n-1}, m, s)A(p_{n-2}, m, s)$. This case is covered by the theorem. We may therefore suppose $n > 3$ and assume by induction on $n-k$ that the corollary is true for $2 \leqq k \leqq n-1$. Let us put $X_k = J(k, m_1, s_1)$ and $Y_k = J(k, m_2, s_2)$. We note that X_k commutes with Y_k if and only if $X_kY_k^{-1} = Y_k^{-1}X_k$. Now

$$X_1 = X_3A(p_2, m_1, s_1)A(p_1, m_1, s_1)$$

and $Y_1 = Y_3A(p_2, m_2, s_2)A(p_1, m_1, s_1)$. Setting $B_{jk} = A(p_j, m_k, s_k)$, $1 \leqq j, k \leqq 2$, we find that

$$X_1Y_1^{-1} = X_3B_{21}B_{11}B_{12}^{-1}B_{22}^{-1}Y_3^{-1}.$$

Now by Theorem 3, $B_{21}B_{11}B_{12}^{-1}B_{22}^{-1} = B_{12}^{-1}B_{22}^{-1}B_{31}B_{11}$ and $B_{12}^{-1}X_3 = X_3B_{12}^{-1}$; moreover, $B_{11}Y_1^{-1} = Y_1^{-1}B_{11}$. Thus $X_1Y_1^{-1} = B_{12}^{-1}X_3B_{22}^{-1}B_{21}Y_3^{-1}B_{11}$, and and since B_{22}^{-1} commutes with B_{21},

$$X_1Y_1^{-1} = B_{12}^{-1}X_2Y_2^{-1}B_{11}.$$

By induction, X_2 commutes with Y_2^{-1}; hence $X_1Y_1^{-1} = Y_1^{-1}X_1$.

6. The normalized principal series. This section is devoted to the construction and study of a series of unitary representations of G which we shall call the normalized principal series. Before describing these representations it will be convenient to make several notational conventions.

Let λ be a continuous unitary character of the diagonal sub-group of G. Then we can write

$$\lambda(c)=\prod_{j=1}^{n}\left(\frac{c_j}{|c_j|}\right)^{m_j}|c_j|^{s_j},\ c\in C \tag{6.1}$$

where $m_1, m_2, \cdots, m_n$ are integers and $s_1, s_2, \cdots, s_n$ are complex numbers such that $Re(s_j)=0$, $1\leqq j\leqq n$. Moreover, we can choose m_j and s_j so that

$$0\leqq\sum_{j=1}^{n}m_j<n \tag{6.2}$$

and

$$\sum_{j=1}^{n}s_j=0. \tag{6.3}$$

Furthermore, this can be done in only one way; that is, (6.1), (6.2), (6.3) determine m_j and s_j uniquely. In what follows, we shall always assume these conditions are satisfied. Therefore, we may write $\lambda=(m_1,\cdots,m_n;s_1,\cdots,s_n)$. Let us also put $m_1+\cdots+m_n=r$ and

$$\operatorname{res}\lambda=(0,\cdots,r;0,\cdots,0). \tag{6.4}$$

We shall call the character $\operatorname{res}\lambda$ the residue of λ. The characters therefore split up into n distinct classes according to their residues.

Let p_k, $1\leqq k\leqq n-1$, be the unitary matrix given by (3.1). We recall that $p_1, p_2, \cdots, p_{n-1}$ generate a finite group S which we have referred to as the Weyl group. If we regard the elements of G as acting by right multiplication on complex n-tuple space then p_k sends $(w_1,\cdots,w_k,w_{k+1},\cdots,w_n)$ into $(w_1,\cdots,-w_{k+1},w_k,\cdots,w_n)$. It follows that S is essentially the symmetric group of degree n. If

$$\lambda=(m_1,\cdots,m_k,m_{k+1},\cdots,m_n;s_1,\cdots,s_k,s_{k+1},\cdots,s_n)$$

then it is easily verified that

$$p_k\lambda=(m_1,\cdots,m_{k+1},m_k,\cdots,m_n;s_1,\cdots,s_{k+1},s_k,\cdots,s_n)$$

where $p_k\lambda(c)=\lambda(p_k^{-1}cp_k)$, $c\in C$. Hence if q is any element of S it follows that λ and $q\lambda$ have the same residue.

If $\lambda=(m_1,\cdots,m_n;s_1,\cdots,s_n)$ denote by $J(k,\lambda)$ the operator $J(k,m_k,s_k)$ defined by (5.17), and set

$$W(\lambda)=J(1,\lambda)J(2,\lambda)\cdots J(n-1,\lambda). \tag{6.5}$$

Furthermore, if $a\rightarrow T(a,\lambda)$ is the representation of the principal series corresponding to λ, let

$$R(a,\lambda)=W(\lambda)T(a,\lambda)W(\lambda)^{-1},\ a\in G. \tag{6.6}$$

Since $W(\lambda)$ is a unitary operator, (6.6) defines a continuous unitary representation $a \to R(a, \lambda)$ of G on $L_2(V)$. These new representations $a \to R(a, \lambda)$ are, by construction, unitarily equivalent to the corresponding representations $a \to T(a, \lambda)$ of the principal series. We shall call this new series of representations the *normalized principal series.*

The following theorem which describes the behaviour of $R(a, \lambda)$ as a function of λ is one of the main results of this paper.

THEOREM 3. *Let G be the complex unimodular group of degree n and Λ the collection of continuous unitary characters of the diagonal sub-group C. Denote by G_0 the sub-group of G which consists of all those elements $a \in G$ with the property that $a_{jn} = 0$, $1 \leqq j \leqq n-1$. If $a \in G$ and $\lambda \in \Lambda$, let $R(a, \lambda)$ be the operator of the normalized principal series defined by* (6.6).

(1) *Then for each fixed $a \in G_0$, $R(a, \lambda)$ as a function of λ depends only upon the residue of λ; in fact*

$$R(a, \lambda) = R(a, \operatorname{res} \lambda) = T(a, \operatorname{res} \lambda) \tag{6.7}$$

where $T(a, \operatorname{res} \lambda)$ is the operator (1.18) *of the principal series, corresponding to the element $a \in G_0$ and to the character* $\operatorname{res} \lambda$, *given by* (6.4).

(2) *In addition,*

$$R(a, \lambda) = R(a, q\lambda) \tag{6.8}$$

for all $a \in G$, $\lambda \in \Lambda$, and q in the Weyl group S.

Remarks. (i) If we allow the elements of G to act as before on complex n-tuple space, then G_0 is the largest sub-group of G leaving invariant the $n-1$ dimensional subspace of vectors $(w_1, \cdots, w_n)$ for which $w_n = 0$. Moreover, in the proof we shall show that a given element of G is either in G_0 or in $G_0 p_{n-1} G_0$. The study of the dependence of $R(a, \lambda)$ on λ for a general element $a \in G$ is therefore reduced by (1) to the study of the operators $R(p_{n-1}, \lambda)$. In particular, the problem of the analytic continuation of the operators $R(a, \lambda)$ to non-unitary characters is essentially reduced to the problem of the continuation of the operators $R(p_{n-1}, \lambda)$.

(ii) Given part (1) of the theorem, part (2) follows from the result of Gelfand and Neumark [3] that the representations of the principal series are irreducible when restricted to G_0. For the representations of the normalized series are then also irreducible on G, and moreover, the representations corersponding to λ and $q\lambda$ are unitarily equivalent. Thus there is a unitary operator $B(\lambda)$ such that

$$B(\lambda)R(a,\lambda)=R(a,q\lambda)B(\lambda),\ a\in G.$$

But since λ and $q\lambda$ have the same residue, $R(a,\lambda)=R(a,q\lambda)$, $a\in G_0$. Hence

$$B(\lambda)R(a,\lambda)=R(a,\lambda)B(\lambda),\ a\in G_0.$$

Because the representations are irreducible on G_0 it follows that $B(\lambda)$ is a non-zero scalar multiple of the identity. Thus $R(a,\lambda)=R(a,q\lambda)$ for all $a\in G$.

On the other hand, it is not difficult to prove (2) directly, and we shall give a proof which does not use the irreducibility of the representations of G_0.

LEMMA 12. *Let S be the group generated by $p_1, p_2, \cdots, p_{n-1}$ and H the lower triangular sub-group,* i. e., *the set of all $a\in G$ such that $a_{jk}=0$ for $j<k$. Then G is a finite union of double cosets of the form HqH where q is an element of S.*

Proof. See Gelfand and Neumark [3].

LEMMA 13. *G_0 is generated (algebraically) by H and $p_1, p_2, \cdots, p_{n-2}$.*

Proof. Let G_0' be the sub-group of G_0 consisting of all elements a such that $a_{nn}=1$ and $a_{nj}=0$, $1\leqq j\leqq n-1$. Then G_0' is isomorphic to $G(n-1)$ and contains $p_1, \cdots, p_{n-2}$. Moreover, it is easily seen that every element of G_0 can be expressed as the product of an element of G_0' with one in H. The lemma follows easily from these observations and the result of Lemma 12 applied to $G(n-1)$.

LEMMA 14. $G=G_0\cup G_0p_{n-1}G_0$.

Proof. Let $a\in G$. Then by Lemma 12 there is an element $q\in S$ such that $a\in HqH$. Let us suppose that a is not a member of G_0. Then Lemma 13 shows that q is not a member of the sub-group S' generated by $p_1, \cdots, p_{n-2}$. It follows that there exist elements q', q'' in S' such that $q=q'p_{n-1}q''$ and hence that $a\in G_0p_{n-1}G_0$. This is most easily seen from the interpretation of of S as the 'symmetric group' together with the following fact about permutations: If π is a permutation of the integers $1, 2, \cdots, n$ which does not fix n then there exist permutations π', π'' fixing n such that $\pi=\pi'(n-1,n)\pi''$ where $(n-1,n)$ denotes the transposition interchanging n and $n-1$.

If w is a non-zero complex number we shall find it convenient, in what follows, to adopt the notational device of writing $[w]$ for $\frac{w}{|w|}$.

LEMMA 15. *Let m be an integer, $Re(s)=0$, and $1 \leqq k \leqq n-1$. Then for each $c \in C$ and $\lambda \in \Lambda$*

$$A(p_k, m, s)T(c,\lambda) = \left[\frac{c_k}{c_{k+1}}\right]^{-m} \left|\frac{c_k}{c_{k+1}}\right|^{-s} T(c,\lambda)A(p_k, m, s). \tag{6.9}$$

Proof. Let ϵ denote the identity character. Then since $\lambda(vc) = \lambda(c)$ for each λ in Λ and v in V it follows that $T(c,\lambda) = \lambda(c)T(c,\epsilon)$. Hence $\lambda(c)T(c,\lambda_1) = \lambda_1(c)T(c,\lambda)$ for all λ, λ_1 in Λ. Using this relation and (4.2) we find that

$$A(p_k,\lambda_1)T(c,\lambda) = \frac{\lambda_1(p_k^{-1}cp_k)}{\lambda_1(c)} \cdot T(c,\lambda)A(p_k,\lambda_1). \tag{6.10}$$

If $\lambda_1 = (m_1, \cdots, m_n; s_1, \cdots, s_n)$ an easy computation shows

$$\frac{\lambda_1(p_k^{-1}cp_k)}{\lambda_1(c)} = \left[\frac{c_k}{c_{k+1}}\right]^{m_{k+1}-m_k} \left|\frac{c_k}{c_{k+1}}\right|^{s_{k+1}-s_k}.$$

In addition, $A(p_k,\lambda_1) = A(p_k, m_k - m_{k+1}, s_k - s_{k+1})$. Now choosing λ_1 so that $m = m_k - m_{k+1}$ and $s = s_k - s_{k+1}$ and substituting into (6.10) we obtain (6.9).

LEMMA 16. *Let $1 \leqq j, k \leqq n-1$, $q = p_j$, and $p = p_k$. If m is an integer and $Re(s) = 0$, let $M(q,m,s)$ be the operator on $L_2(V)$ given by*

$$M(q,m,s)f(v) = [v_{j+1\,j}]^{-m} \, |v_{j+1\,j}|^{-s} f(v). \tag{6.11}$$

In addition, let

$$T(q,m,s) = M(q,m,s)T(q,\epsilon) \tag{6.12}$$

where $T(q,\epsilon)$ is the operator of the principal series corresponding to q, ϵ. Then

$$A(p,m,s)T(p,m,s) = T(p,-m,-s)A(p,m,s); \tag{6.13}$$

$$A(p,m,s)T(q,m',s') = T(q,m',s')A(p,m,s) \text{ if } |k-j| > 1; \tag{6.14}$$

$$A(p,m,s)T(q,m',s') = T(q,m+m',s+s')A(p,m,s) \text{ if } |k-j| = 1. \tag{6.15}$$

Proof. Let $\lambda = (m_1, \cdots, m_n; s_1, \cdots, s_n)$. Then (1.18) and Lemma 2 show that

$$T(q,\lambda) = T(q, m_j - m_{j+1}, s_j - s_{j+1}). \tag{6.16}$$

We also have the relation

$$A(p,\lambda) = A(p, m_k - m_{k+1}, s_k - s_{k+1}).$$

Furthermore,

$$T(p, p\lambda) = T(p, m_{j+1} - m_j, s_{j+1} - s_j).$$

Putting these observations together and using (4.2) we obtain (6.13).

If $|k - j| > 1$ then $T(q, \lambda) = T(q, p\lambda)$ and (6.14) follows immediately from (4.2).

In proving (6.15) we shall suppose $j = k + 1$, the argument being entirely similar in the case $k = j + 1$. If m, s, m', and s' are given we can always choose λ so that $m = m_k - m_{k+1}$, $s = s_k - s_{k+1}$, $m' = m_{k+1} - m_{k+2}$, and $s' = s_{k+1} - s_{k+2}$. Then it is also true that $m + m' = m_k - m_{k+2}$ and $s + s' = s_k - s_{k+2}$. Moreover,

$$T(q, p\lambda) = T(q, m_k - m_{k+2}, s_k - s_{k+2}).$$

From these relations and (4.2) we obtain (6.15).

Proof of Theorem 3. (1) Since $R(a_1a_2, \lambda) = R(a_1, \lambda)R(a_2, \lambda)$ for all a_1, a_2 in G and $\lambda \in \Lambda$, the validity of (6.7) for a_1, a_2 in G_0 implies its validity for their product a_1a_2. Now $H = VC$, and by Lemma 13, G_0 is generated by $p_1, \cdots, p_{n-2}$ and H. Thus it suffices to prove (6.7) when $a \in V$, $a \in C$, and $a = p_j$, $1 \leqq j \leqq n - 2$.

Let us suppose first that $a \in V$. Then in (1.18) $\lambda(va)\mu^{\frac{1}{2}}(va) = 1$ for all $v \in V$. Thus $T(a, \lambda_1) = T(a, \lambda_2)$ for all λ_1, λ_2 in Λ. Using this relation and (4.2) we find that the operators $A(p_k, m, s)$ commute with $T(a, \lambda)$. The operators $J(k, m, s)$ given by (5.17) therefore commute with $T(a, \lambda)$ and hence by (6.5) we see that $W(\lambda)$ also commutes with $T(a, \lambda)$. Thus $R(a, \lambda) = T(a, \lambda)$ and we have established (6.7) in the case that $a \in V$.

We now assume that $a = c \in C$. We also suppose $\lambda = (m_1, \cdots, m_n; s_1, \cdots, s_n)$ and that conditions (6.2) and (6.3) are satisfied. Then rewriting (6.1) we find that

$$\lambda(c) = \prod_{k=1}^{n-1} \left[\frac{c_k}{c_{k+1}}\right]^{\alpha_k} \left|\frac{c_k}{c_{k+1}}\right|^{\beta_k} \operatorname{res} \lambda(c) \tag{6.17}$$

where

$$\alpha_k = m_1 + \cdots + m_k$$

$$\beta_k = s_1 + \cdots + s_k.$$

Now let us observe that the operator $J(j, m_j, s_j)$, defined by (5.17), contains $A(p_k, m_j, s_j)$ as a factor if and only if $j \leqq k \leqq n - 1$. Thus the factors of the form $A(p_k, m, s)$ in the product (6.5) are precisely those of the form $A(p_k, m_j, s_j)$, $1 \leqq j \leqq k$. It therefore follows from (6.9) that

$$W(\lambda)T(c, \lambda)W(\lambda)^{-1} = \frac{\operatorname{res} \lambda(c)}{\lambda(c)} T(c, \lambda).$$

Hence $W(\lambda)T(c, \lambda)W(\lambda)^{-1} = T(c, \operatorname{res} \lambda)$.

We shall now prove (6.7) for $a = p_j$ where $1 \leqq j \leqq n-2$. Since $1 \leqq j \leqq n-2$, we see from (6.16) that $T(p_j, \operatorname{res}\lambda) = T(p_j, \epsilon)$. Thus it will suffice to show that

$$W(\lambda)T(p_j,\lambda) = T(p_j,\epsilon)W(\lambda). \tag{6.18}$$

Let $\lambda = (m_1, \cdots, m_n; s_1, \cdots, s_n)$. Then by (6.16),

$$T(p_j,\lambda) = T(p_j, m_j - m_{j+1}, s_j - s_{j+1})$$

and by (6.14)

$$J(k,\lambda)T(p_j,\lambda) = T(p_j,\lambda)J(k,\lambda),\ j+1 < k \leqq n-1. \tag{6.19}$$

From (6.15) and (6.13) we see that

$$J(j+1,\lambda)T(p_j,\lambda) = T(p_j, m_j, s_j)J(j+1,\lambda). \tag{6.20}$$

Using (6.13), (6.15), and (6.14) we now find that

$$J(j,\lambda)T(p_j, m_j, s_j) = T(p_j,\epsilon)J(p,\lambda). \tag{6.21}$$

By similar computations with (6.13), (6.14), and (6.15) we also find that

$$J(k,\lambda)T(p_j,\epsilon) = T(p_j,\epsilon)J(k,\lambda),\ 1 \leqq k < j. \tag{6.22}$$

Finally, we observe that (6.18) is implied by equations (6.19) through (6.22).

(2) If (6.8) holds for q_1, q_2 in S, then using the fact that $(q_1q_2)\lambda = q_1(q_2\lambda)$ for all λ we see that it is also valid for q_1q_2. It therefore suffices to prove (6.8) for the generators, p_k of S. Suppose then that k is fixed and let $p = p_k$. Then $R(a,\lambda) = R(a, p\lambda)$ if and only if

$$W(\lambda)T(a,\lambda)W(\lambda)^{-1} = W(p\lambda)T(a,p\lambda)W(p\lambda)^{-1}.$$

This condition is equivalent, however, to the condition that

$$W(p\lambda)^{-1}W(\lambda)T(a,\lambda) = T(a,p\lambda)W(p\lambda)^{-1}W(\lambda).$$

To prove this it will suffice, in view of (4.2), to show that $A(p,\lambda) = W(p\lambda)^{-1}W(\lambda)$. We shall prove the equivalent condition

$$W(p\lambda) = W(\lambda)A(p,\lambda)^{-1}. \tag{6.23}$$

Now $A(p_k,\lambda) = A(p_k, m_k - m_{k+1}, s_k - s_{k+1})$ and hence by Lemma 3

$$\begin{aligned} A(p_k,\lambda)^{-1} &= A(p_k, m_{k+1}, s_{k+1})A(p_k, -m_k, -s_k) \\ &= A(p_k, -m_k, -s_k)A(p_k, m_{k+1}, s_{k+1}). \end{aligned} \tag{6.24}$$

Thus $J(n-1,\lambda)A(p_{n-1},\lambda)^{-1}=J(n-1,p_{n-1}\lambda)$, and when $1\leqq j\leqq n-2$, $J(j,\lambda)=J(j,p_{n-1}\lambda)$. It follows from (6.5) that (6.23) holds when $k=n-1$. Now suppose $1\leqq k\leqq n-2$. Then

$$J(k+1,m_{k+1},s_{k+1})A(p_k,m_{k+1},s_{k+1})=J(k,m_{k+1},s_{k+1}).$$

It follows from (6.24) that

$$J(k,\lambda)J(k+1,\lambda)A(p_k,\lambda)^{-1}=J(k,m_k,s_k)J(k,m_{k+1},s_{k+1})A(p_k,-m_k,-s_k).$$

Furthermore, the corollary to Theorem 2 shows that $J(k,m_k,s_k)$ commutes with $J(k,m_{k+1},s_{k+1})$, and since $J(k,m_k,s_k)A(p_k,-m_k,-s_k)=J(k+1,m_k,s_k)$ we see that

$$J(k,\lambda)J(k+1,\lambda)A(p_k,\lambda)^{-1}=J(k,p_k\lambda)J(k+1,p_k\lambda). \tag{6.25}$$

In addition, $A(p_k,\lambda)^{-1}$ commutes with $J(j,\lambda)$ when $k+1<j\leqq n-1$, and $J(j,\lambda)=J(j,p_k\lambda)$ whenever $|k-j|>1$. From these observations and (6.25) we conclude that $W(p_k\lambda)=W(\lambda)A(p_k,\lambda)^{-1}$.

7. Lemmas on analytic continuation of certain operators. The results of this section as well as those of the next will be used in Section 9 to construct uniformly bounded representations of G. The main idea of this construction is to continue the operators $R(a,\lambda)$, of the normalized principal series, analytically in the parameters specifying λ.

We begin by recalling some standard definitions and results concerning analytic operator valued functions. Let H be a Hilbert space and $s\to P(s)$ a function defined in a domain D of the complsx plane whose values are bounded operators on H. Then $P(\cdot)$ is said to be analytic in D if $s\to(P(s)f,g)$ is analytic in D for all f, g in H. By a well known theorem of Hille ([7]; p. 53) such a function is continuous in the uniform operator norm and has a complex derivative, again in the uniform norm. From this it follows that if $P(\cdot)$ and $Q(\cdot)$ are analytic operator valued functions in D, then so is their product $s\to P(s)Q(s)$.

LEMMA 17. *Let $\gamma(m,s)$ be defined by (3.5) and $s=a+ib$. Then there is a constant K independent of m and s such that*

$$\frac{1}{|\gamma(m,s)|}<K(1+|m|+|b|)^{1-a},\quad -1<a<1. \tag{7.1}$$

Proof. Let $c=\dfrac{|m|+2}{2}$ and $z=\dfrac{s}{2}=x+iy$. Then

$$\frac{i^{|m|}\pi 2^s}{\gamma(m,s)}=\frac{\Gamma(c-z)}{\Gamma(c-1+z)}=(c-1+z)\frac{\Gamma(c-z)}{\Gamma(c+z)}.$$

To estimate the factor $\frac{\Gamma(c-z)}{\Gamma(c+z)}$ we use Stirling's formula (see Titchmarsh [10; p. 151]) which implies that $\log\Gamma(w)-(w-\frac{1}{2})\log w+w$ is uniformly bounded in any sector of the form $-\pi+\epsilon\leqq\arg w\leqq\pi-\epsilon$ (for fixed $\epsilon>0$) the logarithms being principal values. In this connection we also make use of the following easily verified estimates.

$$|(c-z-\tfrac{1}{2})\log\left(\frac{c-z}{c-iy}\right)|\leqq|x|,\ -\tfrac{1}{2}<x<\tfrac{1}{2}. \tag{7.2}$$

$$|(c+z-\tfrac{1}{2})\log\left(\frac{c+z}{c+iy}\right)|\leqq|x|,\ -\tfrac{1}{2}<x<\tfrac{1}{2}. \tag{7.3}$$

From (7.2), (7.3), and Stirling's formula we find that

$$\begin{aligned}&\log\Gamma(c-z)-\log\Gamma(c+z)\\ &\qquad=-2z\log|c-iy|+i(2c-1)\arg(c-iy)+2z+B(z)\end{aligned} \tag{7.4}$$

where $B(z)$ is uniformly bounded in $-\frac{1}{2}<Re(z)<\frac{1}{2}$. At this point it is a straighforward matter to derive (7.1) from (7.4).

In the next three lemmas we shall be concerned with the analytic continuation of various combinations of the operators $A(m,s)$ and $B(m,s)$ treated in the last part of Section 5 (cf. equations (5.9), (5.10), and Lemma 11.)

LEMMA 18. *Let m be a fixed integer and $L_2=L_2(v)$ where v is one complex variable. Then the operator $A(m,s)\cdot B(m,s)$ initially defined on L_2 for $Re(s)=0$ can be continued into the strip $0\leqq Re(s)<1$ in such a way that*

(1) *for each f, g in L_2 the function*

$$s\to(A(m,s)B(m,s)f,g)$$

is analytic in $0<Re(s)<1$ and continuous in $0\leqq Re(s)<1$.

(2) $$\|A(m,s)B(m,s)\|\leqq K_d(1+|m|+|b|)^{1-a}$$

where $s=a+ib$, $0\leqq a\leqq d<1$, and $\|\cdot\|$ denotes the usual operator norm.

Remark. Part of the interest of this result lies in the fact that the natural continuations of $A(m,s)$ and $B(m,s)$ are unbounded operators for $0<Re(s)<1$, but nevertheless their product $A(m,s)B(m,s)$ remains bounded.

Proof. Let D denote the linear space of all bounded, compactly supported functions in L_2 which also vanish in a neighborhood of the origin. If f and g belong to D and $Re(s) = 0$ let

$$\Phi(f, g, s) = (A(m, s)B(m, s)f, g).$$

Then since $A(m, s)^* = A(-m, \bar{s})$ (see Lemma 3) it follows that

$$\Phi(f, g, s) = (B(m, s)f, A(-m, \bar{s})g).$$

Next we shall define $\Phi(f, g, s)$ when $0 < Re(s) < 1$. To do this we first put

$$B(m, s)f(v) = \left(\frac{v}{|v|}\right)^{-m} |v|^{-s} f(v), \; 0 \leqq Re(s) < 1. \tag{7.5}$$

Then $B(m, s)f \in L_2$, and if $f(v) = 0$ when $|v| < \delta$ it follows that $|B(m, s)f| \leqq \delta^{-1} |f|$. Hence, by dominated convergence, $s \rightarrow B(m, s)f$ is continuous in $0 \leqq Re(s) < 1$ as a function with values in L_2. By Lemma 3, $s \rightarrow A(-m, \bar{s})g$ is also continuous as a function from $0 \leqq Re(s) < 1$ into L_2. Thus setting

$$\Phi(f, g, s) = (B(m, s)f, A(-m, \bar{s})g), \; 0 \leqq Re(s) < 1 \tag{7.6}$$

we see that $\Phi(f, g, s)$ is continuous in $0 \leqq Re(s) < 1$. Furthermore, $\Phi(f, g, s)$ is uniformly bounded in any strip of the form $0 \leqq Re(s) \leqq d$, $0 < d < 1$. For the explicit form of the Fourier transform of $A(-m, \bar{s})g$, which is given in the proof of Lemma 3, shows that

$$\| A(-m, \bar{s})g \|_2 \leqq \| A(-m, a)g \|_2, \quad s = a + ib, 0 \leqq a < 1.$$

Thus in $0 \leqq Re(s) \leqq d$

$$|\Phi(f, g, s)| \leqq \delta^{-1} \|f\|_2 \cdot \sup_{0 \leqq a \leqq d} \| A(-m, a)g \|_2 < \infty. \tag{7.7}$$

The bound given in (7.7) is of course dependent on f and g.

We now suppose $0 < Re(s) < 1$, and in order to simplify the notation we shall as before write $[v]$ for $\frac{v}{|v|}$. Then from (7.6), (7.5), (5.9), and the fact that $\bar{\gamma}(-m, \bar{s}) = (-1)^m \gamma(m, s)$ we find that

$$\gamma(m, s)\Phi(f, g, s) = \int [v]^{-m} |v|^{-s} f(v)\, dv \int [z]^m |z|^{-2+s} \bar{g}(v + z)\, dz.$$

In the integral with respect to z, we make the transformation $z \rightarrow vz - v$ and obtain

$$\gamma(m, s)\Phi(f, g, s) = \int f(v)\, dv \int [z - 1]^m |z - 1|^{-2+s} \bar{g}(zv)\, dz. \tag{7.8}$$

Thus

$$|\gamma(m, s)\Phi(f, g, s)| \leqq \int |f(v)|\, dv \int |z - 1|^{-2+s} |g(zv)|\, dz$$

where $s = a + ib$ and $0 < a < 1$. Now setting

$$h(v) = \int |z-1|^{-2+a} |g(zv)| \, dz$$

and using Minkowski's inequality for integrals we find that

$$\| h \|_2 \leqq \int |z-1|^{-2+a} [\int |g(zv)|^2 \, dv]^{\frac{1}{2}} \, dz = K_a' \| g \|_2$$

where $K_a' = \int |z-1|^{-2+a} |z|^{-1} \, dz$ and is uniformly bounded in any closed interval contained in $(0,1)$. In fact K_a' is continuous as a function of a in the open interval $(0,1)$. Thus

$$\int |f(v)| \, dv \int |z-1|^{-2+a} |g(zv)| \, dz \leqq K_a' \| f \|_2 \| g \|_2$$

and setting

$$F(s) = \int f(v) \, dv \int [z-1]^m |z-1|^{-2+s} \bar{g}(zv) \, dz, \; 0 < Re(s) < 1$$

we find that the integrals defining F are absolutely convergent in $0 < Re(s) < 1$. Moreover, because of the boundedness of K_a', Fubini's theorem shows that

$$\int_\Delta F(s) \, dx = 0$$

for every triangle Δ contained in the strip $0 < Re(s) < 1$. Thus F is analytic in $0 < Re(s) < 1$. Now in view of the analyticity of $1/\gamma(m,s)$ and (7.8) it follows that $\Phi(f,g,s)$ is analytic in $0 < Re(s) < 1$. If $Re(s) = 0$ and s is fixed, the definition of Φ shows that

$$f, g \to \Phi(f,g,s)$$

is a sesqui-linear form on D. Thus, since $s \to \Phi(f,g,s)$ is analytic in $0 < Re(s) < 1$ and continuous in $0 \leqq Re(s) < 1$, for fixed f, g in D, we see that

$$f, g \to \Phi(f,g,s)$$

is also sesqui-linear when $0 < Re(s) < 1$. This follows because a function G is identically 0 if it is analytic in $0 < Re(s) < 1$, continuous in $0 \leqq Re(s) < 1$, and vanishes when $Re(s) = 0$.

Next we shall obtain a bound for Φ. First of all we see from Lemma 17 and the estimates given above that

$$|\Phi(f,g,s)| \leqq K_a (1 + |m| + |b|)^{1-a} \| f \|_2 \| g \|_2 \tag{7.9}$$

where $s = a + ib$, $0 < a < 1$, and K_a is independent of f and g; however, K_a

does not remain bounded as $a \to 0$. In order to get around this difficulty we shall use a standard Phragmén-Lindelöf argument.

We fix d so that $0 < d < 1$. Then in (7.9) we may assume without loss of generality that $K_d \geqq 1$. Now consider the function Φ_1 defined by

$$\Phi_1(s) = K_d^{-1}(1 + |m| + s)^{a-1}(\|f\|_2 \|g\|_2)\Phi(f, g, s), \quad 0 \leqq Re(s) < 1.$$

When $Re(s) = 0$, the operators $B(m, s)$ and $A(-m, \bar{s})$ are unitary. Hence from (7.6) we find that $|\Phi(f, g, s)| \leqq \|f\|_2 \|g\|_2$, $Re(s) = 0$. Therefore

$$|\Phi_1(s)| \leqq 1, \; Re(s) = 0.$$

And from (7.9) it follows that

$$|\Phi_1(s)| \leqq 1, \; Re(s) = d.$$

In addition, (7.7) shows that $\Phi(f, g, s)$ is uniformly bounded in $0 \leqq Re(s) \leqq d$; thus Φ_1 is also uniformly bounded in $0 \leqq Re(s) \leqq d$. We conclude that $|\Phi_1(s)| \leqq 1$, $0 \leqq Re(s) \leqq d$. This shows that (7.9) can be replaced by the stronger estimate

$$(7.10) \qquad \begin{aligned} &|\Phi(f, g, s)| \leqq K_d(1 + |m| + |b|)^{1-a} \|f_2\| \, \|g\|_2, \\ &\qquad\qquad s = a + ib, \; 0 \leqq a \leqq d < 1. \end{aligned}$$

Since (7.10) holds for a dense class of functions f, g there is for each s in $0 < Re(s) < 1$, a unique sesqui-linear form

$$f, g \to \Phi_1(f, g, s)$$

defined for all f, g in L_2 which extends

$$f, g \to \Phi(f, g, s)$$

and satisfies (7.10). Because the uniform limit of continuous (analytic) functions is still continuous (analytic) the function

$$s \to \Phi_1(f, g, s)$$

is continuous in $0 \leqq Re(s) < 1$ and analytic in $0 < Re(s) < 1$, for each f, g in L_2. Let $A(m, s)B(m, s)$ denote the operator on L_2 which is defined by $\Phi_1(\cdot, \cdot, s)$. It is then apparent that the operator valued function $s \to A(m, s)B(m, s)$ satisfies (1) and (2). This concludes the proof of the lemma.

We now define another operator $C(m, m', s, s')$ on $L_2 = L_2(v)$, where v is one complex variable, by setting

$$
\begin{aligned}
&C(m, m', s, s') \\
&\quad = A(m, s) B(m + m', s + s') - B(m + m', s + s') A(m, s).
\end{aligned}
\tag{7.11}
$$

Here we assume that $Re(s) = Re(s') = 0$ and that m and m' are integers.

LEMMA 19. *Let m, m' and s' be fixed. Then the operator $C(m, m', s, s')$, initially defined on L_2 for $Re(s) = 0$, can be continued into the strip $-1 < Re(s) < 1$ in such a way that*

(1) *for each f, g in L_2 the function*

$$s \rightarrow (C(m, m', s, s') f, g)$$

is analytic in $-1 < Re(s) < 1$, and

(2) $\| C(m, m', s, s') \| \leqq K_a (1 + | m | + | m' | + | b | + | b' |)^{2-a}$

where $\| \cdot \|$ denotes the usual operator norm, $s = a + ib$, $s' = ib'$, and $-1 < a < 1$.

Proof. The proof is similar to part of the proof of Lemma 18, and we shall therefore omit some of the details. We begin with functions f, g both of which are bounded, vanish outside a bounded set, and are 0 in a neighborhood of the origin. For such functions f, g we put

$$
\begin{aligned}
(f, g, s) &= (B(m + m', s + s') f, A(-m, \bar{s}) g) \\
&\qquad - (A(m, s) f, B(-m, -m', -\bar{s} + \bar{s}') g)
\end{aligned}
\tag{7.12}
$$

where $0 \leqq Re(s) < 1$. Then

$$\Phi(f, g, s) = (C(m, m', s, s') f, g)$$

when $Re(s) = 0$. On the other hand when $0 < Re(s) < 1$ we find, by rewriting the integrals, that

$$
\begin{aligned}
&\gamma(m, s) \Phi(f, g, s) \\
&= \int \int [z - v]^m \, | z - v |^{-2+s} f(v) \bar{g}(z) ([v]^{-m-m'} \, | v |^{-s-s'} - [z]^{-m-m'} \, | z |^{-s-s'}) \, dv dz.
\end{aligned}
$$

Now by means of the transformation $v \rightarrow zv$, $z \rightarrow z$ we obtain the relation

$$
\begin{aligned}
&\gamma(m, s) \Phi(f, g, s) \\
&= [z]^{-m'} \, | z |^{-s'} \int \int [1 - v]^m \, | 1 - v |^{-2+s} f(zv) \bar{g}(z) ([v]^{-m-m'} \, | v |^{-s-s'} - 1) \, dv dz
\end{aligned}
\tag{7.13}
$$

which holds when $0 < Re(s) < 1$. We shall show next that the integral in (7.13) converges absolutely whenever f, g belong to L_2 and $-1 < Re(s) < 1$.

Let I_1 denote the integral over the set where $|v-1| \leqq \frac{1}{2}$ and I_2 the integral over the complementary set. To estimate I_1 we use the inequality

$$(7.14) \qquad |[v]^{-m-m'}|v|^{-s-s'}-1| \leqq K(1+|m+m'|+|b+b'|)|v-1|$$

which is valid for $|v-1| \leqq \frac{1}{2}$, $s=a+ib$, $s'=ib'$, and $-1<a<1$. It follows from (7.14) that

$$|I_1| \leqq K(1+|m+m'|+|b+b'|)\int\int_{|v-1|\leqq\frac{1}{2}} |f(zv)\bar{g}(z)|\,|v-1|^{-1+a}dvdz.$$

By Minkowski's inequality for integrals,

$$|I_1| \leqq K(1+|m+m'|+|b+b'|)\|f\|_2\|g\|_2\int\int_{|v-1|\leqq\frac{1}{2}} |v-1|^{-1+a}|v|^{-1}\,dv$$

$$= K_a(1+m+m'|+|b+b'|)\|f\|_2\|g\|_2, -1<a.$$

Now consider I_2. Notice that

$$|1-[v]^{-m-m'}|v|^{-s-s'}| \leqq 1+|v|^{-a}, \quad s=a+ib$$

and that

$$|v-1|^{-2+a} \leqq K(1+|v|)^{-2+a}, \quad |v-1| \geqq \tfrac{1}{2}.$$

Hence

$$|I_2| \leqq K(1+|m+m'|+|b+b'|)$$

$$\int\int_{|v-1|\geqq\frac{1}{2}} |f(vz)g(z)|(1+|v|)^{-2+a}(1+|v|^{-a})dvdz.$$

Moreover

$$\int\int |f(vz)g(z)|(1+|v|)^{-2+a}(1+|v|^{-a})dvdz$$

$$\leqq \|f\|_2\|g\|_2\int|v|^{-1}(1+|v|)^{-2+a}(1+|v|^{-a})dv$$

and $\int|v|^{-1}(1+|v|)^{-2+a}(1+|v|^{-a})dv<\infty$ if $a<1$. These estimates show that the integral in (7.13) is bounded by

$$K_a(1+|m+m'|+|b+b'|)\|f\|_2\|g\|_2$$

for $-1<a<1$ and all f,g in L_2. Furthermore, the above argument, in which we obtained the estimates for $|I_1|$ and $|I_2|$, can easily be modified to show that the integral in (7.13) is analytic as a function of s in $-1<Re(s)<1$. From (7.12) it follows that $\Phi(f,g,s)$ is continuous in $0\leqq Re(s)<1$. Hence we may use the integral in (7.13) to define

$\gamma(m,s)\Phi(f,g,s)$ for $-1 < Re(s) < 1$. Then from the above estimates and Lemma 17 we conclude that

$$(7.15) \quad |\Phi(f,g,s)| \leqq K_a(1+|m|+|m'|+|b|+|b'|)^{2-a} \|f\|_2 \|g\|_2.$$

for $-1 < a < 1$ and all f, g in L_2. Thus statements (1) and (2) of the lemma are satisfied by the operator $C(m,m',s,s')$ which is defined by the form $\Phi(\cdot,\cdot,s)$.

Next we define another operator by setting

$$(7.16) \quad E(m,m',s,s') = A(m,s)B(m+m',s+s')A(-m,-s)B(-m,-s).$$

Here we assume that m and m' are integers and that $Re(s) = Re(s') = 0$.

LEMMA 20. *Let m, m' and s' be fixed. Then the operator $E(m,m',s,s')$, initially defined on L_2 for $Re(s) = 0$, can be continued into the strip $-1 < Re(s) < 1$ in such a way that*

(1) *for each f, g in L_2, the function*

$$s \to (E(m,m',s,s')f,g)$$

is analytic in $-1 < Re(s) < 1$, and

(2) $\|E(m,m',s,s')\| \leqq K_a(1+|m|+|m'|+|b|+|b'|)^3$

where $s = a+ib$, $s' = ib'$, and $-1 < a < 1$.

Proof. If $Re(s) = 0$, (7.11) shows that

$$A(m,s)B(m+m',s+s') = C(m,m',s,s') + B(m+m',s+s')A(m,s).$$

Hence rewriting (7.16) we find that

$$E(m,m',s,s') = C(m,m',s,s')A(-m,-s)B(-m,-s) + B(m',s').$$

In view of the two preceding lemmas we may now extend the definition of $E(m,m',s,s')$ by setting

$$(7.17) \quad E(m,m',s,s') = C(m,m',s,s')A(-m,-s)B(-m,-s) + B(m',s'), \quad -1 < Re(s) \leqq 0.$$

On the other hand when $Re(s) = 0$, it is possible to rewrite (7.16) in another way. For it is easy to see that

$$A(m,s)B(m+m',s+s') \cdot C(-m,-m',-s,-s') = E(m,m',s,s')B(-m',-s') - I.$$

Hence

$$E(m, m', s, s')$$
$$= A(m, s)B(m, s) \cdot B(m', s')C(m, m', s, s')B(m', s') + B(m', s').$$

By Lemmas 18 and 19, the right side of this equation is well defined for $0 \leqq Re(s) < 1$. We shall put

$$(7.18) \quad E(m, m', s, s')$$
$$= A(m, s)B(m, s) \cdot B(m', s')C(-m, -m', -s, -s')B(m', s') + B(m', s'),$$
$$0 \leqq Re(s) < 1.$$

To prove (1) let us suppose f and g are fixed functions in L_2. Let

$$\Phi_+(s) = (E(m, m', s, s')f, g), \quad 0 \leqq Re(s) < 1.$$

Also let

$$P(s) = A(m, s)B(m, s) \quad \text{and} \quad Q(s) = B(m', s')C(-m, -m', -s, -s')B(m', s').$$

It follows from Lemmas 18 and 19 that $P(s)$ and $Q(s)$ are analytic in $0 < Re(s) < 1$, and hence so is their product $s \rightarrow P(s)Q(s)$. From (7.18) we conclude that Φ_+ is also analytic in $0 < Re(s) < 1$. Now suppose $Re(s_0) = 0$. Then

$$(P(s)Q(s)f, g) = (P(s)Q(s_0)f, g) + (Q(s)f - Q(s_0)f, P(s)^*g)$$

and Lemma 18 shows that $(P(s)Q(s_0)f, g) \rightarrow (P(s_0)Q(s_0)f, g)$ as $s \rightarrow s_0$. On the other hand, it also shows that $\| P(s) \|$ is uniformly bounded in every compact subset of $0 \leqq Re(s) < 1$. Hence, since $Q(s)$ is uniformly continuous

$$|(Q(s)f - Q(s_0)f, P(s)^*g)| \leqq K \| Q(s) - Q(s_0) \| \, \| f \|_2 \, \| g \|_2 \rightarrow 0$$

as $s \rightarrow s_0$. It follows that Φ_+ is continuous in $0 \leqq Re(s) < 1$. Next we put

$$\Phi_-(s) = (E(m, m', s, s')f, g), \quad -1 < Re(s) \leqq 0.$$

Then, by arguments similar to those just given, it follows that Φ_- is analytic in $-1 < Re(s) < 0$ and continuous in $-1 < Re(s) \leqq 0$. Since $\Phi_+(s) = \Phi_-(s)$ when $Re(s) = 0$, Φ_+ and Φ_- are analytic continuations of each other. This proves (1). Finally, we observe that (2) follows from (7.17), (7.18), the fact that $B(m', s')$ is unitary, and the bounds given in Lemmas 18 and 19.

8. Some lemmas on several complex variables.

The first result we prove here is similar to well known theorems (cf. Bochner and Martin, *Several*

Complex Variables) on the analytic continuation of functions of several complex variables, but deals with functions initially defined on a set which is considerably thinner than those which appear to have been treated in the literature.

LEMMA 21. *Let $G(z_1, z_2, \cdots, z_m)$ be a given function of m variables $(z_j = x_j + iy_j)$, initially defined and continuous on the set where $Re(z_j) = 0$, $j = 1, 2, \cdots, m$. Suppose that for every fixed j, and fixed $iy_1, iy_2, \cdots, iy_{j-1}, iy_{j+1}, \cdots, iy_m$*

$$G(iy_1, \cdots, iy_{j-1}, z_j, iy_{j+1}, \cdots, iy_m)$$

as a function of z_j is analytically extendable into the strip $|Re(z_j)| < 1$ and satisfies $|G| \leqq 1$ there. Then G is extendable into the tube

$$|x_1| + |x_2| + \cdots + |x_m| < 1 \quad (y\text{'s arbitrary})$$

is analytic there, as a function of the m variables, and satisfies $|G| \leqq 1$ there.

Proof. Let $G(iy_1, iy_2, \cdots, iy_m) = G(iy)$ and $D_j = \frac{1}{i}\frac{\partial}{\partial y_j}$. It then follows easily from our assumptions that for each j

$$\sup_{y} |D_j^n G(iy)| \leqq n!, \quad n = 0, 1, 2, \cdots. \tag{8.1}$$

Let $H(z) = (2 - z_1)^{-2}(2 - z_2)^{-2} \cdots (2 - z_m)^{-2}$. Then

$$D_j^k H(iy) = \frac{(k+1)!}{(2 - iy_j)^k} \cdot H(iy).$$

Now putting $F(iy) = G(iy)H(iy)$, we find that

$$D_j^n F(iy) = H(iy) \cdot \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} \cdot \frac{(k+1)!}{(2 - iy_j)^k} \cdot D_j^{n-k} G(iy).$$

Hence by (8.1) and simple estimates

$$|D_j^n F(iy)| \leqq (n+1)! \, |H(iy)|. \tag{8.2}$$

Let $f(\lambda) = \int e^{i\langle y, \lambda\rangle} F(iy)\, dy$ where $\langle y, \lambda\rangle = y_1\lambda_1 + y_2\lambda_2 + \cdots + y_m\lambda_m$. Then integrating by parts, we find that

$$\lambda_j^n f(\lambda) = \int e^{i\langle y, \lambda\rangle} D_j^n F(iy)\, dy.$$

Thus in view of (8.2) and the fact that H is integrable, there is a constant A such that

$$\sup_{\lambda} |\lambda_j^n f(\lambda)| \leqq A(n+1)!, \quad n = 0, 1, 2, \cdots. \tag{8.3}$$

It follows that F can be expressed in terms of f by means of the Fourier inversion formula. Thus

$$F(iy) = \frac{1}{(2\pi)^m}\int e^{-i\langle y,\lambda\rangle} f(\lambda)\,d\lambda.$$

Next we set

$$F(x+iy) = \frac{1}{(2\pi)^m}\int e^{-\langle x+iy,\lambda\rangle} f(\lambda)\,d\lambda.$$

We shall show that this integral converges absolutely whenever $x+iy$ is in the tube described above. Let x be fixed and such that $\sum_j |x_j| = \mu < 1$. Then for each λ, $|\langle x,\lambda\rangle| \leqq \mu \max|\lambda_j|$. Thus

$$\int e^{-\langle x,\lambda\rangle} |f(\lambda)|\,d\lambda \leqq \sum_n \frac{\mu^n}{n!}\int \max|\lambda_j|^n\,|f(\lambda)|\,d\lambda.$$

Now using (8.3), we see that

$$\int \max|\lambda_j|^n\,|f(\lambda)|\,d\lambda \leqq A(n+m+2)!\int \frac{d\lambda}{1+\max|\lambda_j|^{m+1}}$$
$$\leqq K(n+m+2)! < \infty.$$

Since the series

$$\sum_n K\cdot\frac{(n+m+2)!}{n!}\cdot\mu^n$$

is convergent, it follows that

$$\int e^{-\langle x,\lambda\rangle}\,|f(\lambda)|\,d\lambda < \infty.$$

Thus the integral in (8.4) is absolutely convergent, and the function $F(z) = F(z_1, z_2, \cdots, z_m)$, which it defines, is analytic in the tube $\sum |Re(z_j)| < 1$. We now set

$$G(z) = \frac{F(z)}{H(z)},\quad \sum |Re(z_j)| < 1.$$

Then G is an analytic extension of our original function into the tube. To show that $|G| \leqq 1$ we suppose that there is some point z_0 such that $|G(z_0)| > 1$. We then consider the function

$$\tilde{G}(iy) = \frac{A}{w - G(iy)}$$

where $w = G(z_0)$ and A is chosen so that $\operatorname{Sup}_y |\tilde{G}(iy)| \leqq 1$. The function $\tilde{G}$ then satisfies our original conditions on G but obviously cannot be extended so as to be analytic at z_0. Hence $|G| \leqq 1$.

LEMMA 22. *Let T be a linear map of $\boldsymbol{C}^m$ to $\boldsymbol{C}^p$ such that $T(\boldsymbol{R}^m) = \boldsymbol{R}^p$, and let Γ be the tube in $\boldsymbol{C}^m$ consisting of all $z = x + iy$ such that $\sum |x_j| < 1$. Suppose G is an analytic function defined on Γ with the property that $G(iy) = G(iy')$ whenever $Ty = Ty'$. Then there is a unique analytic function F defined on $T(\Gamma)$ such that*

$$F(Tz) = G(z),\ z \in \Gamma. \tag{8.5}$$

Proof. We may suppose the null space of T has dimension k where $k > 0$. Then since $T(\boldsymbol{R}^m) \subset T(\boldsymbol{R}^p)$ there is a linear map $w \to \tilde{w}$ of $\boldsymbol{R}^k$ onto the null space of T which sends real vectors into real vectors. Fix $v \in \boldsymbol{R}^k$ and for $a \in \Gamma$, let $H(z) = G(z + i\tilde{v}) - G(z)$. Then H is analytic in Γ and $H(iy) = 0$ for all $y \in \boldsymbol{R}^m$. Since Γ is a tube and is both open and connected, it follows by analytic continuation that

$$G(z + i\tilde{v}) = G(z),\ z \in \Gamma. \tag{8.6}$$

Now fix $z \in \Gamma$ and let

$$\Gamma_z = \{w \in \boldsymbol{R}^k \colon \tilde{w} + z \in \Gamma\}.$$

Then Γ_z is an open connected tube in $\boldsymbol{R}^k$ which contains the set $Re(w) = 0$. In Γ_z we define a function K by setting $K(w) = G(z + i\tilde{w}) - G(z)$. Then K is analytic in Γ_z and by (8.6) $K(iv) = 0$ for all $v \in \boldsymbol{R}^k$. Thus, by analytic continuation, we see that $G(z + \tilde{w}) = G(z)$ for all $w \in \Gamma_z$. In other words, $G(z) = G(z')$ whenever z and z' belong to Γ and $Tz = Tz'$. It follows that there is a unique well defined function F on $T(\Gamma)$ which satisfies (8.5). Furthermore, our assumptions on T imply that $T(\Gamma)$ is an open convex tube in $\boldsymbol{C}$. Now let s' be a fixed vector in $T(\Gamma)$. Then there exists a vector z' in Γ and a non-singular linear map L of $\boldsymbol{C}^p$ into $\boldsymbol{C}^m$ such that $Ls' = z'$ and TL is the identity on $\boldsymbol{C}^p$. If s is sufficiently close to s', $F(s) = G(Ls)$. It follows that F is analytic in a neighborhood of s' and hence that F is analytic in $T(\Gamma)$.

In our application we shall not use Lemma 21 directly but a slight variant of it. We shall be concerned with a function $F(s_1, s_2, \cdots, s_n)$ initially defined in a subset of the complex hyperplane $s_1 + s_2 + \cdots + s_n = 0$. Our problem as before, will be to extend F so that it is analytic in a larger set. We shall say a function defined on a subset of $s_1 + s_2 + \cdots + s_n = 0$ is analytic if it is analytic in the usual sense as a function of the $n-1$ complex variables $s_1, s_2, \cdots, s_{n-1}$ (with $s_n = -s_1 - s_2 - \cdots - s_{n-1}$). Before stating our result it will be convenient to introduce some notation. Let $0 < d \leq 1$, $s_j = a_j + ib_j$ and $B(d)$ denote the smallest convex set in the real hyperplane $a_1+a_2+\cdots+a_n=0$ which contains the points $(a,-a,0,\cdots,0)$, $-d<a<d$, and all permutations of these points.

Now let $\mathcal{T}(d)$ denote the tube in $s_1+s_2+\cdots+s_n=0$ whose basis is $B(d)$, i.e., the set of all points $(a_1+ib_1,\cdots,a_n+ib_n)$ where $(a_1,a_2,\cdots,a_n)\in B(d)$ and $b_1+b_2+\cdots+b_n=0$, but otherwise the b's are arbitrary. Then $\mathcal{T}(d)$ is an open convex subset of $s_1+s_2+\cdots+s_n=0$, and with these conventions our result can be formulated in the following way.

LEMMA 23. *Let F be defined and continuous on the set where $s_1+s_2+\cdots+s_n=0$ and $a_j=0$, $j=1,2,\cdots,n$. Moreover, suppose that for every pair j,k, $1\leqq j<k\leqq n$ and fixed $ib_1,ib_2,\cdots,ib_n$ (such that $\sum b_j=0$) the function*

$$F_{jk}(s)=F(ib_1,\cdots,ib_j+s,\cdots,ib_k-s,\cdots,ib_n)$$

as a function of the one complex variable $s=a+ib$ has an analytic extension into the strip $-d<Re(s)<d$ and $|F_{jk}(s)|\leqq 1$ there. Then F has an analytic extension to the tube $\mathcal{T}(d)$ which satisfies the condition $|F|\leqq 1$.

Proof. Set $m=\dfrac{n(n-1)}{2}$, label the coordinates of points $z=x+iy$ in $\boldsymbol{C}^m$ with two indices jk, $1\leqq j<k\leqq n$, and let $\bar{T}$ be the linear map of $\boldsymbol{C}^m$ onto the hyperplane $s_1+s_2+\cdots+s_n=0$ which is given by the equations

$$s_j=d\sum_{k>j}z_{jk}-d\sum_{k<j}z_{kj},\quad 1\leqq j\leqq n.$$

Put $G(iy)=F(i\bar{T}y)$. Then it is easily seen that Lemma 22 applies to G and hence that G can be extended analytically into the tube Γ whose basis is the set $\sum|x_j|<1$. Now let $p=n-1$ and T be the map $\bar{T}$ followed by the projection $(s_1,s_2,\cdots,s_n)\to(s_1,s_2,\cdots,s_{n-1})$. Applying Lemma 22 and the observation that $\bar{T}(\Gamma)=\mathcal{T}(d)$, we easily obtain the conclusion of Lemma 24.

9. Analytic continuation of the normalized principal series. In this section we consider the problem of the analytic continuation of the representations $a\to R(a,\lambda)$ which are intially defined for unitary characters by (6.6). We shall obtain, in the end, a larger family of uniformly bounded representations, some of which are again unitary (the complementary series) and others which are not.

Let $\mathcal{T}$ be the 'tube' $\mathcal{T}(1)$ which is described in the paragraph preceding

Lemma 23. We denote by Λ^* the set of all characters λ of the diagonal subgroup C of G having the form

$$\lambda(c) = \prod_{j=1}^{n} \left(\frac{c_j}{|c_j|} \right) |c_j|^{s_j}, \ c \in C \tag{9.1}$$

where $m_1, m_2, \cdots, m_n$ are integers and $s_1, s_2, \cdots, s_n$ are complex numbers satisfying

(i) $0 \leqq \sum m_j < n$,

(ii) $(s_1, s_2, \cdots, s_n) \in \mathcal{F}$.

We shall use the notation

$$\lambda = (m_1, m_2, \cdots, m_n; s_1, s_2, \cdots, s_n)$$

for the character given by (9.1).

It is clear that Λ^* contains the set of all continuous unitary characters of C, i. e., those which in addition to the above satisfy the condition $Re(s_j) = 0$, $j = 1, 2, \cdots, n$. As in Section 6, we shall denote the set of unitary characters by Λ.

A given complex or operator valued function

$$F(\lambda) = F(m_1, m_2, \cdots, m_n; s_1, s_2, \cdots, s_n)$$

defined on Λ^* will be called *analytic* if for fixed $m_1, m_2, \cdots, m_n$ it is complex analytic as a function of $s_1, s_2, \cdots, s_{n-1}$.

Having made these conventions we are now in a position to state our main theorem.

THEOREM 4. *Let G be the complex unimodular group of degree n, C its diagonal sub-group, Λ the collection of continuous unitary characters of C, and Λ^* the larger collection defined by* (9.1). *If $a \in G$ and $\lambda \in \Lambda$, let $R(a, \lambda)$ be the operator of the normalized principal series given by* (6.6). *Then for each fixed $a \in G$, the operator valued function*

$$\lambda \rightarrow R(a, \lambda)$$

initially defined on Λ can be extended into Λ^* in such a way that

(1) *it is analytic in Λ^*;*

(2) *for each fixed $\lambda \in \Lambda^*$*

$$a \rightarrow R(a, \lambda), \ a \in G$$

is a continuous uniformly bounded representation of G *on* $L_2(V)$, V *being the group of lower triangular unipotent matrices in* G;

(3) *if* S *is the Weyl group, the representations* $a \to R(a,\lambda)$ *are invariant under* S *in the sense that*

$$R(a, q\lambda) = R(a, \lambda)$$

for all $a \in G$, $\lambda \in \Lambda^*$, *and* $q \in S$, *where* $q\lambda$ *is the element of* Λ^* *given by*

$$(q\lambda)(c) = \lambda(q^{-1}cq), \quad c \in C.$$

(4) *if the contragredient of a character in* Λ^* *or an operator on* $L_2(V)$ *is denoted by a prime then*

$$R(a, \lambda') = R(a, \lambda)'$$

for all $a \in G$ *and all* $\lambda \in \Lambda^*$.

Remarks. (i) In the proof of (2) we obtain an explicit but by no means best possible bound for the representation $a \to R(a,\lambda)$. Our estimate may be described as follows: Let $\lambda = (m_1, m_2, \cdots, m_m; s_1, s_2, \cdots, s_n) \in \Lambda^*$. Then there is a real number d such that $0 < d < 1$ and $-d < Re(s_j) < d$, $j = 1, 2, \cdots, n$. We show that

$$\operatorname*{Sup}_{a \in G} \| R(a,\lambda) \| \leqq K_d' \,| H(\lambda) |$$

where $\|\cdot\|$ denotes the usual operator norm, K_d' is independent of λ, and $H(\lambda)$ is the analytic function on Λ^* defined by (9.9).

(ii) Let $\lambda \in \Lambda^*$ and $a \in G$. Then $\lambda'(c) = \bar{\lambda}(c^{-1})$, $c \in C$ and $R(a,\lambda)'$ is the adjoint of $R(a,\lambda)^{-1}$. Thus λ is unitary if and only if $\lambda = \lambda'$, and in this case, statement (4) simply says that the representations of the normalized principal series are unitary. On the other hand, it is well known that G has another series of unitary representations, the so-called complementary series whose members are determined by certain non-unitary characters of C.

In the present situation, we obtain the complementary series, more precisely representations unitarily equivalent to the complementary series, in a very simple fashion. In fact the following result is an immediate consequence of (3) and (4) above.

COROLLARY. *Let* $\lambda \in \Lambda^*$ *and suppose there is an element* $q \in S$ *such that* $\lambda' = q\lambda$. *Then* $a \rightarrow R(a, \lambda)$ *is a unitary representation of* G.[8]

In the proof of the theorem we shall need a number of lemmas.

LEMMA 24. *Let* $p = p_{n-1}$ *where* p_{n-1} *is the element of the Weyl group defined by* (3.1). *For* $Re(s) = 0$ *and*

$$\lambda = (m_1, m_2, \cdots, m_n; ib_1, ib_2, \cdots, ib_n) \in \Lambda,$$

let

$$Q(\lambda, s) = R(p, m_1, \cdots, m_n; ib_1, \cdots, ib_{n-1} + s, ib_n - s). \tag{9.2}$$

Then for fixed λ, *the operator* $Q(\lambda, s)$ *can be continued into the strip* $-1 < Re(s) < 1$, *in such a way that*

(1) *for each* f, g *in* $L_2(V)$, *the function*

$$s \rightarrow (Q(\lambda, s)f, g)$$

is analytic in $-1 < Re(s) < 1$, *and*

(2) $\| Q(\lambda, s) \| \leqq K_a(1 + (\Sigma \,|\, m_j \,| + |\, b_j \,|) + |\, b \,|)^3$

where $s = a + ib$, $-1 < a < 1$.

Proof. By (6.6),

$$R(p, \lambda) = W(\lambda)T(p, \lambda)W(\lambda)^{-1} \text{ where } W(\lambda) = J(1, \lambda)J(2, \lambda) \cdots J(n-1, \lambda)$$

and

$$J(k, \lambda) = A(p_{n-1}, m_k, ib_k) \cdots A(p_{k+1}, m_k, ib_k)A(p_k, m_k, ib_k). \tag{9.3}$$

Let us put

$$W_1(\lambda) = J(1, \lambda) \cdots J(n-2, \lambda), T_1(p, \lambda) = J(n-1, \lambda)T(p, \lambda)J(n-1, \lambda)^{-1},$$

and

$$Q_1(\lambda, s) = T_1(p, m_1, \cdots, m_n; ib_1, \cdots, ib_{n-1} + s, ib_n - s). \tag{9.4}$$

---

[8] That these representations are unitarily equivalent to the representations of the complementary series may be seen as follows: The two pairs of representations have the same characters as may be seen from formula (10.4) and the trace formula on page 115 of [3]. Thus it follows by a theorem of Harish-Chandra in [6] that the representations are untarily equivalent.

Then $R(p,\lambda) = W_1(\lambda)T_1(p,\lambda)W_1(\lambda)^{-1}$, and it follows from (9.3) that $W_1(\lambda)$ is independent of ib_{n-1}; in fact, $W_1(\lambda) = W_1(m_1, \cdots, m_{n-2}; ib_1, \cdots, ib_{n-2})$. Thus

$$Q(\lambda, s) = W_1(\lambda)Q_1(\lambda, s)W_1(\lambda), \ Re(s) = 0. \tag{9.5}$$

Since $W_1(\lambda)$ is independent of s and unitary, it will suffice to prove statements (1) and (2) of the lemma for Q_1 instead of Q. In doing this, we first note that

$$\begin{aligned} T(p,\lambda) &= T(p, m_{n-1} - m_n, ib_{n-1} - ib_n) \\ &= M(p, -m_n, -b_n)T(p, m_{n-1}, ib_{n-1}) \end{aligned}$$

where $M(p, -m_n, -ib_n)$ and $T(p, m_{n-1}, ib_{n-1})$ are given by (6.11) and (6.12) respectively. To simplify the notation we set

$$m_{n-1} = m, \ b_{n-1} = b, \ m' = -m_{n-1} - m_n, \text{ and } b' = -b_{n-1} - b_n.$$

Then by the multiplicative properties of M

$$T(p,\lambda) = M(p, m + m', ib + ib')T(p, m, ib).$$

Thus $T_1(p,\lambda) = A(p, m, ib)B(p, m + m', ib + ib')T(p, m, ib)A(p, -m, -ib)$. Moreover, (6.13) and (6.12) show that

$$\begin{aligned} T(p, m, ib)A(p, -m, -ib) &= A(p, -m, -ib)T(p, -m, -ib) \\ &= A(p, -m, -ib)M(p, -m, -ib)T(p, \epsilon). \end{aligned}$$

Now setting

$$\begin{aligned} (9.6)\quad & L(m, m', ib, ib') \\ &= L(m, m', ib, ib') \\ &= A(p, m, ib)M(p, m + m', ib + ib')A(p, -m, -ib)M(p, -m, -ib) \end{aligned}$$

it follows that $T_1(p,\lambda) = L(m, m', ib, ib')T(p,\epsilon)$. Since $b' = -b_{n-1} - b_n$, i.e., since $b' = b_1 + \cdots + b_{n-2}$, we see from (9.4) that

$$Q_1(\lambda, s) = L(m, m', ib_{n-1} + s, ib')T(p, \epsilon), \ Re(s) = 0. \tag{9.7}$$

Let us consider the operator $L(m, m', ib_{n-1}, ib')$. To study its action we use (as in the proof of Lemma 3, Section3) the decomposition

$$L_2(V) = L_2(Z \times Z'), \quad Z = Z(n-1, n).$$

We recall that this representation of $L_2(V)$ arises from the expression of V as the semi-direct product ZZ' and that Z is isomorphic to the additive group of complex numbers. If $f \in L_2(V)$ we can therefore write $f(v) = f(z, z')$. Let us suppose that $f(z, z') = g(z)h(z')$ where $g \in L_2(Z)$ and $h \in L_2(Z')$. It is then easily verified that

$$L(m, m', ib_{n-1}, ib')f(z, z') = E(m, m', ib_{n-1}, ib')g(z) \cdot h(z') \tag{9.8}$$

where $E(m, m', ib_{n-1}, ib')$ is the operator defined by (7.16).

Hence upon applying Lemma 20, we see that $E(m, m', ib_{n-1} + s, ib')$ can be continued so as to be analytic in $-1 < Re(s) < 1$. In addition

$$\| E(m, m', ib_{n-1} + s, ib') \| \leqq K_a(1 + | m | + | m' | + | b_{n-1} + b | + | b' |)^3$$

where $s = a + ib$ and $-1 < a < 1$. It now follows easily from (9.8) that $L(m, m', ib_{n-1} + s, ib')$ can be continued so as to be analytic in $-1 < Re(s) < 1$ with the same (operator) bound as $E(m, m', ib_{n-1} + s, ib')$. In view of (9.7) and the fact that $T(p, \epsilon)$ is unitary the same can be said of $Q_1(\lambda, s)$. To obtain the bound given in (2), we need only observe that $| m | + | m' | \leqq 2(\sum | m_j |)$ and that $| b' | \leqq \sum | b_j |$. This concludes the proof of the lemma.

Since we frequently need to refer to the following elementary result, we shall state it as a lemma.

LEMMA 25. *Let F_1 and F_2 be analytic complex or operator valued functions defined on Λ^*. Then $F_1 = F_2$ if $F_1(\lambda) = F_2(\lambda)$ for all $\lambda \in \Lambda$.*

LEMMA 26. *Let $H(\lambda) = H(m_1, m_2, \cdots, m_n; s_1, s_2, \cdots, s_n)$ be defined for $\lambda \in \Lambda^*$ by*

$$H(\lambda) = (1 + \sum_j | m_j |)^3 \prod_j (3 - s_j)^6. \tag{9.9}$$

If $0 < d < 1$ let $\Lambda^*(d)$ denote the set of all $\lambda \in \Lambda^*$ such that $-d < Re(s_j) < d$, $j = 1, 2, \cdots, n$. Then the operator valued function $R(p, \lambda)$ initially defined for $\lambda \in \Lambda$ can be continued into Λ^* in such a way that

(1) *for each f, g in $L_2(V)$, the function*

$$\lambda \to (R(p, \lambda)f, g)$$

is analytic in Λ^*, and

$$\| R(p, \lambda) \| \leqq K_d' \, | H(\lambda) |, \quad \lambda \in \Lambda^*(d) \tag{2}$$

where K_d' is independent of λ.

Proof. Let $\lambda = (m_1, \cdots, m_n; ib_1, \cdots, ib_n) \in \Lambda$. Then if $-1 < Re(s) < 1$ we shall put

$$\lambda_s = (m_1, \cdots, m_n; ib_1, \cdots, ib_{n-1} + s, ib_n - s).$$

It follows that $\lambda_s \in \Lambda^*$. Now in view of (9.2) and Lemma 24 we may extend the domain of definition of $R(p, \lambda)$ by setting

$$R(p, \lambda_s) = Q(\lambda, s), \quad -1 < Re(s) < 1. \tag{9.10}$$

Next we define our operator for permutations of λ_s. To be specific, let us suppose $k_1, k_2, \cdots, k_n$ is a permutation of $1, 2, \cdots, n$. Then there is an element q of the Weyl group, i.e., an element q of S such that

$$q\lambda = (m_{k_1}, \cdots, m_{k_n}; ib_{k_1}, \cdots, ib_{k_n}).$$

By Theorem 3, $R(p, \lambda) = R(p, q\lambda)$ for all λ in Λ. We may therefore obtain an extension of our operator, which is invariant under S, by setting

$$R(p, q \cdot \lambda_s) = R(p, \lambda_s), \quad -1 < Re(s) < 1. \tag{9.11}$$

From the bound given in Lemma 24 it is easy to see that $\| Q(\lambda, s) \| \leqq K_a | H(\lambda) |$. Thus since H is invariant under permutations it follows at once from (9.10) that

$$\| R(p, q \cdot \lambda_s) \| \leqq K_a | H(q \cdot \lambda_s) |$$

To simplify the notation, let Λ' denote the set of all characters of the form $q \cdot \lambda_s$, $\lambda \in \Lambda$, $q \in S$. *Then* Λ' can also be described as the set of all characters in Λ^* of the form

$$\lambda = (m_1, \cdots, m_n; ib_1, \cdots, ib_j + s, \cdots, ib_k - s, \cdots, ib_n) \tag{9.12}$$

where $1 \leqq j < k \leqq n$ and $-1 < Re(s) < 1$. At this point we have succeeded in defining $R(p, \lambda)$ for all characters λ in Λ'. Furthermore we have the bound

$$\| R(p, \lambda) \| \leqq K_a | H(\lambda)) \tag{9.13}$$

where λ has the form (9.12) and $s = a + ib$. If f and g belong to $L_2(V)$ and $\lambda \in \Lambda'$ we set

$$\Phi(f, g, \lambda) = (R(p, \lambda) f, g). \tag{9.14}$$

If $0 < d < 1$ and $K_d' = \sup_{-d<a<d} K_a$ it follows from (9.13) that

$$|\Phi(f,g,\lambda)| \leqq K_d' \, |H(\lambda)| \, \| f \|_2 \, \| g \|_2 \tag{9.15}$$

for all $\lambda \in \Lambda' \cap \Lambda^*(d)$, i.e., all λ if the form (9.12) where $-d < Re(s) < d$. Next we fix f and g and show that $\Phi(f,g,\lambda)$, as a function of λ, can be extended analytically into $\Lambda^*(d)$. In doing this, we may of course assume that $\| f \|_2 \, \| g \|_2 \neq 0$. We put

$$F(\lambda) = \frac{\Phi(f,g,\lambda)}{K_d' \cdot H(\lambda) \cdot \| f \|_2 \, \| g \|_2}, \quad \lambda \in \Lambda' \cap \Lambda^*(d).$$

Then for fixed $m_1, \cdots, m_n$ and fixed $b_1, b_2, \cdots, b_n$ the function

$$F_{jk}(s) = F(m_1, \cdots, m_n; ib_1, \cdots, ib_j + s, \cdots, ib_k - s, \cdots, ib_n)$$

is analytic in $-d < Re(s) < d$. This follows from Lemma 24, (9.10), (9.11), (9.14), and the fact that $1/H$ is analytic in Λ^*. Furthermore F_{jk} is bounded by 1. It now follows from Lemma 24 that F has an analytic extension into $\Lambda^*(d)$ which is also bounded by 1. Thus $\Phi(f,g,\lambda)$ has an analytic extension to $\Lambda^*(d)$ which satisfies (9.15). Moreover, since

$$\Lambda^* = \bigcup_{0<d<1} \Lambda^*(d)$$

our argument shows that $\Phi(f,g,\lambda)$ can be extended into Λ^*. If $\lambda \in \Lambda$ is fixed, it follows from (9.14) that $f, g \rightarrow \Phi(f,g,\lambda)$ is a sesqui-linear form on $L_2(V)$. By Lemma 25 the same is true for any fixed $\lambda \in \Lambda^*$. In addition

$$|\Phi(f,g,\lambda)| \leqq K_d' \, |H(\lambda)| \, \| f \|_2 \, \| g \|_2$$

for all λ in $\Lambda^*(d)$. Therefore, $\Phi(\cdot,\cdot,\lambda)$ defines for each $\lambda \in \Lambda^*$, a bounded operator which we denote by $R(p,\lambda)$. It is then clear that $R(p,\lambda)$ satisfies statements (1) and (2) of the lemma.

Proof of Theorem 4. (1) Let $\lambda = (m_1, m_2, \cdots, m_n; s_1, s_2, \cdots, s_n) \in \Lambda^*$, and $r = \sum m_j$. Then, extending the definition given in Section 6, we shall put

$$\operatorname{res} \lambda = (0, \cdots, r; 0, \cdots, 0)$$

and call $\operatorname{res} \lambda$ the residue of λ. Suppose now that $a \in G_0$, the sub-group of all elements a such that $a_{jn} = 0$, $1 \leqq j \leqq n-1$. Then in view of Theorem 3, we may define $R(a,\lambda)$ in a consistent, in fact analytic, fashion by setting

$$R(a,\lambda) = R(a, \operatorname{res} \lambda). \tag{9.16}$$

On the other hand if $a \in G$ and is not a member of G_0, then, by Lemma 14, $a \in G_0 p G_0$ where $p = p_{n-1}$. We can then write $a = bpb'$ with b and b' in G_0. By (9.16) and Lemma 26, the function

$$\lambda \rightarrow R(b,\lambda)R(p,\lambda)R(b',\lambda)$$

is analytic in Λ^*. In addition

$$R(a,\lambda) = R(b,\lambda)R(p,\lambda)R(b',\lambda), \ \lambda \in \Lambda. \tag{9.17}$$

It follows from Lemma 25 and (9.17) that the function

$$\lambda \rightarrow R(b,\lambda)R(p,\lambda)R(b',\lambda)$$

depends only on a and not on the particular choice of b and b'. It is therefore natural to extend the definition of $R(a,\lambda)$ by setting

$$R(a,\lambda) = R(b,\lambda)R(p,\lambda)R(b',\lambda)$$

for each $\lambda \in \Lambda^*$.

(2) Let a and b belong to G. Then by (1), $R(a,\lambda)$, $R(b,\lambda)$, and $R(ab,\lambda)$ are all analytic, as functions of λ, in Λ^*. Since the product of two analytic operator valued functions in again analytic, $R(a,\lambda)R(b,\lambda)$ is analytic in Λ^*. Furthermore,

$$R(a,\lambda)R(b,\lambda) = R(ab,\lambda) \tag{9.18}$$

whenever $\lambda \in \Lambda$. Applying Lemma 25 we see that (9.18) holds for all $\lambda \in \Lambda^*$. This shows $a \rightarrow R(a,\lambda)$ is a representation.

Next we show that when λ is fixed the operators $R(a,\lambda)$ are uniformly bounded as functions of $a \in G$. If $a \in G_0$, then $R(a,\lambda)$ is unitary and hence $\| R(a,\lambda) \| = 1$. On the other hand, if $a \in G$ and is not in G_0, $a = bpb'$, as above, with b, b' in G_0. It follows that $\| R(a,\lambda) \| = \| R(p,\lambda) \|$, and for the bound of $R(p,\lambda)$ we have the estimate given by Lemma 26.

Now suppose f, g are fixed functions in $L_2(V)$ and that $\{a_k\}$ is a sequence of elements in G tending to the identity. Let us consider the sequence of functions

$$F_k(\lambda) = (R(a_k,\lambda)f, g), \ \lambda \in \Lambda^*.$$

We shall show that for each fixed λ, there is a subsequence F_{k_i} such that $F_{k_i}(\lambda) \rightarrow (f, g)$. From this it is easy to conclude that for each fixed λ,

$a \to (R(a,\lambda)f, g)$ is continuous, and this being true for each f, g it will follow that $a \to R(a,\lambda)$ is (weakly) continuous. If

$$\lambda = (m_1, m_2, \cdot \cdot \cdot, m_m; s_1, s_2, \cdot \cdot \cdot, s_n) \in \Lambda^*$$

then we can find d, d' so that

$$(9.19) \qquad -d < Re(s_j) < \mathrm{d}, \ -d' < I_m(s_j) < d', \ 1 \leqq j \leqq n.$$

Let $\Lambda(m_1, m_2, \cdot \cdot \cdot, m_m; d, d')$ be the set of all characters in Λ^* of the form

$$\lambda = (m_1, m_2, \cdot \cdot \cdot, m_n; s_1, s_2, \cdot \cdot \cdot, s_n)$$

which satisfy (9.19). Now fix $m_1, m_2, \cdot \cdot \cdot, m_n$, d and d' and set $\Lambda' = \Lambda(m_1, m_2, \cdot \cdot \cdot, m_n; d, d')$. Then from the bound given in Lemma 27, it follows that there is a constant K independent of k such that

$$(9.20) \qquad | F_k(\lambda) | \leqq K. \ \lambda \in \Lambda'.$$

Since the functions F_k are analytic in Λ' and satisfy (9.20) they are equicontinuous there. Hence there is a subsequence F_{k_i} which converges uniformly on Λ' to a function F which is also analytic in Λ'. We shall show that $F(\lambda) = (f,g)$ for all $\lambda \in \Lambda'$. To do this we make use of the known fact that the representations of the principal series are continuous. From this and (6.6) we see that $a \to R(a,\lambda)$ is continuous whenever λ is a unitary character, i.e., when $\lambda \in \Lambda$. Hence $F_k(\lambda) \to (f,g)$, if $\lambda \in \Lambda$. In particular, this implies $F(\lambda) = (f,g)$ for all $\lambda \in \Lambda \cap \Lambda'$. Thus by analytic continuation we see that $F(\lambda) = (f,g)$ for all $\lambda \in \Lambda'$.

(3) Let a be fixed in G and q an element of S. Then $R(a, q\lambda)$ is analytic as a function of λ and so is $R(a,\lambda)$; in addition(these functions agree when $\lambda \in \Lambda$. By Lemma 25, $R(a, q\lambda) = R(a,\lambda)$ for all $\lambda \in \Lambda^*$.

(4) Suppose a is a fixed element of G. Then to prove $R(a,\lambda') = R(a,\lambda)'$ we must show that $R(a,\lambda') = R(a^{-1},\lambda)^*$. Let $f, g \in L_2(V)$, and put $F(\lambda) = (R(a,\lambda)g, f)$. Then F is analytic in Λ^*, and if $\lambda = (m_1, m_2, \cdot \cdot \cdot, m_n; s_1, s_2, \cdot \cdot \cdot, s_n)$

$$\bar{F}(\lambda')) = \bar{F}(m_1, m_2, \cdot \cdot \cdot, m_n; -\bar{s}_1, -\bar{s}_2, \cdot \cdot \cdot, -\bar{s}_n).$$

It follows easily that $\bar{F}(\lambda')$ is analytic, as a function of λ, in Λ^*. In addition

$$(9.21) \qquad \bar{F}(\lambda') = (f, R(a,\lambda')g), \ \lambda \in \Lambda^*.$$

On the other hand, if λ is unitary then $\lambda = \lambda'$ and $R(a, \lambda) = R(a^{-1}, \lambda)^*$. Thus we have the relation

$$(9.22) \qquad (R(a^{-1}, \lambda)f, g) = (f, R(a, \lambda')g), \ \lambda \in \Lambda.$$

Since both sides of (9.22) are analytic in Λ^* (as functions of λ), it follows from Lemma 25 that (9.22) holds for all $\lambda \in \Lambda^*$. This being true for every f and g in $L_2(V)$. we conclude that $R(a^{-1}, \lambda)^* = R(a, \lambda')$, $\lambda \in \Lambda^*$.

10. Traces and equivalences. In the first theorem of this section we obtain a generalization of a trace formula due to Gelfand and Neumark, [3: p. 93]. With the aid of this formula we then determine the conditions under which two representations of our family

$$a \to R(a, \lambda), \ \lambda \in \Lambda^*$$

are equivalent. In particular we show that not all of our representations are equivalent to unitary representations.

We begin by recalling some rather standard facts. If $\mathfrak{H}$ is a Hilbert space and A is a bounded operator on $\mathfrak{H}$, the L_p norm of A is defined by the equation

$$(10.1) \qquad \| A \|_p = [\operatorname{trace}(A^*A)^{p/2}]^{1/p}, \ 1 \leqq p < \infty$$

and $\| A \|_\infty$ *is* the usual operator norm, $\| A \|$. If $\| A \|_1 < \infty$ then $\operatorname{tr}(A) = \operatorname{trace}(A)$ exists, $|\operatorname{tr}(A)| \leqq \| A \|_1$, and A is said to be of trace class. On the other hand, if A and B are any two bounded operators on $\mathfrak{H}$ then

$$(10.2) \qquad \| AB \|_p \leqq \| A \|_\infty \| B \|_p, \ 1 \leqq p \leqq \infty.$$

Next, let $\lambda \in \Lambda^*$ and $a \in G$. If a has distinct characteristic values $c_1, c_2, \cdots, c_n$ let $c = [c_1, c_2, \cdots, c_n]$ and

$$(10.3) \qquad \psi(a, \lambda) = \sum_p \frac{\lambda(p^{-1}cp)}{D(a)}$$

where $D(a) = \prod_{j<k} | c_j - c_k |^2$ and p ranges over S. If a does not have distinct characteristic values set $\psi(a, \lambda) = 0$. Then $\psi(a, \lambda)$ is a well defined measurable function of a.

THEOREM 5. *Let f be the convolution of two bounded functions with compact support on G. For each $\lambda \in \Lambda^*$, let*

$$R(f,\lambda) = \int_G R(a,\lambda) f(a)\, da.$$

Then $R(f,\lambda)$ is of trace class and

$$\operatorname{tr} R(f,\lambda) = \int_G \psi(a,\lambda) f(a)\, da \tag{10.4}$$

where $\psi(a,\lambda)$ is defined by (10.3).

Equation (10.4) is a generalization of the formula of Gelfand and Neumark [3: p. 93].

THEOREM 6. *Let λ_1 and λ_2 belong to Λ^*, and suppose A is a bounded operator on $L_2(V)$ with a bounded inverse such that*

$$R(a,\lambda_1) = AR(a,\lambda_2)A^{-1}, \quad a \in G.$$

Then there is an element q in the Weyl group, S such that $\lambda_1 = q\lambda_2$, and then, by Theorem 4, $R(a,\lambda_1) = R(a,\lambda_2)$, $a \in G$.

On the other hand, suppose $\lambda \in \Lambda^*$ and that

$$a \to AR(a,\lambda)A^{-1}$$

is a unitary representation, where again A is a bounded operator on $L_2(V)$ with a bounded inverse. Then $a \to R(a,\lambda)$ is already a unitary representation, and there is an element q in S such that $\lambda' = q\lambda$. Thus if $\lambda' \neq q\lambda$ for all $q \in S$, $a \to R(a,\lambda)$ is not equivalent to a unitary representation.

For the proofs of these theorems we require a series of lemmas.

LEMMA 27. *Let U be a compact group and $u \to R(u)$ a continuous representation of U on a Hilbert space $\mathfrak{H}$. Suppose*

$$\sup_{u \in U} \| R(u) \| \leqq M.$$

Then there exists a bounded invertible operator B on $\mathfrak{H}$ such that

(1) $\| B \| \leqq M$, $\| B^{-1} \| \leqq M$, *and*

(2) $u \to BR(u)B^{-1}$ *is a unitary representation of* U.

Proof. Let $x \in \mathfrak{H}$ and suppose $\| x \| = 1$. Then for $u \in U$,

$$\frac{1}{M^2} \leqq (R^*(u)R(u)x, x) \leqq M^2.$$

Hence if $A = \int_U R^*(u)R(u)\,du$ and the measure of U is properly normalized

$$\frac{1}{M^2} \leqq (Ax, x) \leqq M^2.$$

If B is the positive square root of A then $\| B \| \leqq M$ and $\| B^{-1} \| \leqq M$ as well. Part (2) now follows by the usual argument [2].

LEMMA 28. *Let f be a bounded function with compact support on G*

$$R(f, \lambda) = \int_G f(a)R(a, \lambda)\,da, \quad \lambda \in \Lambda^*$$

and

$$K_\lambda = \sup_{a \in G} \| R(a, \lambda) \|.$$

Then $\| R(f, \lambda) \|_2 < K_\lambda{}^6 J_f$ where J_f is a constant depending only on f and not on λ.

This is the key lemma.[9]

Proof. Recall that $R(a, \lambda) |_{G_0}$ is unitary and irreducible.[10] Hence $R(a, \lambda)$ is completely irreducible in the terminology of Godement [5]. Let U be the unitary sub-group of G, and $u \rightarrow D(u)$ a continuous irreducible representation of U. Let $n(D)$ be the number of times that D occurs in the reduction of $R(a, \lambda) |_U$. Then since $R(a, \lambda)$ is completely irreducible it follows from a theorem of Godement [5: Theorem 2] that $n(D) \leqq$ degree (D). Moreover, by Lemma 27, there exists a bounded operator B_λ such that $\| B_\lambda \| \leqq K_\lambda$, $\| B_\lambda{}^{-1} \| \leqq K_\lambda$, and

$$P(a, \lambda) = B_\lambda R(a, \lambda) B_\lambda{}^{-1}$$

is unitary when restricted to U. Since $\| P(a, \lambda) \| \leqq \| B_\lambda \| \, \| R(a, \lambda) \| \, \| B_\lambda{}^{-1} \|$, it follows that

$$\sup_{a \in G} \| P(a, \lambda) \| \leqq K_\lambda{}^3,$$

---

[9] The proof makes use of ideas occurring in paper [6] of Harish-Chandra.

[10] See (9.16), Theorem 3 and subsequent remarks. This is the first place where we use the irreducibility of the principal series on G_0.

Because $P(a,\lambda)$ is equivalent to $R(a,\lambda)$, $n(D)$ is also the number of times D occurs in the reduction of $P(a,\lambda)\,|_U$.

Now let S be the closure of the support of f. Then S is compact and so is $U\cdot S$. Fixing λ and setting $P(a) = P(a,\lambda)$ we then have

$$P_f = \int_G f(a)P(a)\,da = \int_U du \int_G f(ua)P(ua)\,da.$$

From this it follows that

$$\| P_f \|_2 = \| \int_G da \int_U f(ua)P(ua)\,du \|_2 \leqq \int_G \| \int_U f(ua)P(ua)\,du \|_2\, da.$$

Hence, since $\int_U f(ua)P(ua)\,du = (\int_U f(ua)P(u)\,du)P(a)$ it follows from (10.2) that

$$\| P_f \|_2 \leqq \sup_{a\in G} \| P(a) \|_\infty \int_G \| \int_U f(ua)P(u)\,du \|_2\, da.$$

We now estimate $\| \int_U f(ua)P(u)\,du \|_2$. Let $u \to L(u)$ be the left regular representation of U. Then D occurs exactly degree (D) times in L. Since $n(D) \leqq$ degree (D) it follows that

$$\| \int_U f(ua)P(u)\,du \|_2 \leqq \| \int_U f(ua)L(u)\,du \|.$$

In addition, the Peter-Weyl theorem shows that

$$\| \int_U f(ua)L(u)\,du \|_2 = (\int_U | f(ua) |^2\, du)^{\frac{1}{2}} \leqq \sup_{b\in G} | f(b) |.$$

Hence because f has its support in S

$$\begin{aligned}\int_G \| \int_U f(ua)P(u)\,du \|_2\, da &= \int_{U\cdot S} \| \int_U f(ua)P(u)\,du \|_2\, da\\ &\leqq \| f \|_\infty \operatorname{meas}\,(U\cdot S)\\ &= J_f.\end{aligned}$$

Combining these estimates we find that

$$\| P_f \|_2 \leqq K_\lambda{}^8 J_f.$$

However, $R(f,\lambda) = B_\lambda{}^{-1} P_\lambda B_\lambda$. Thus

$$\| R(f,\lambda) \|_2 \leqq \| B_\lambda{}^{-1} \|_\infty \| P_f \|_2 \| B_\lambda \|_\infty \leqq K_\lambda{}^5 J_f$$

which proves the lemma.

LEMMA 29. *Let $f = f_1 * f_2$ where f_1 and f_2 are bounded functions with compact support on G. Then for each $\lambda \in \Lambda^*$*

$$R(f,\lambda) = \int_G f(a) R(a,\lambda)\, da$$

is of trace class, $\| R(f,\lambda) \|_1 \leqq K_\lambda{}^{10} J_f{}'$, and

$$\lambda \to \operatorname{tr} R(f,\lambda)$$

is analytic in Λ^*.

Proof. Since $f = f_1 * f_2$, $R(f,\lambda) = R(f_1,\lambda) R(f_2,\lambda)$. Hence $\| R(f,\lambda) \|_1 \leqq \| R(f_1,\lambda) \|_2 \| R(f_2,\lambda) \|_2$, by Schwarz's inequality, which is valid in the present situation. The preceding lemma now shows that

$$\| R(f,\lambda) \|_1 \leqq K_\lambda{}^{10} J_{f_1} J_{f_2} = K_\lambda{}^{10} J_f{}'.$$

Thus $\operatorname{tr} R(f,\lambda)$ is well defined.

Let $g_1, g_2, \cdots,$ be a fixed orthonormal basis for $L_2(V)$, and let P_n be the orthogonal projection on the subspace spanned by $g_1, g_2, \cdots, g_n$. Then if A is any operator on $L_2(V)$ of trace class we know that

$$\operatorname{tr}(A) = \lim_{n \to \infty} \operatorname{tr}(P_n A P_n)$$

and $| \operatorname{tr}(P_n A P_n) | \leqq \| A \|_1$. Furthermore

$$\operatorname{tr}(P_n A P_n) = \sum_{k=1}^{n} (A g_k, g_k). \tag{10.5}$$

Now let $F_n(\lambda) = \operatorname{tr}(P_n R(f,\lambda) P_n)$ and $F(\lambda) = \operatorname{tr}(R(f,\lambda))$. In view of

(10.5) and the fact that $\lambda \to R(a,\lambda)$ is analytic in Λ^*, and hence that $\lambda \to R(f,\lambda)$ is analytic there, it follows that F_n is analytic in Λ^*. We also have the estimate

$$|F_n(\lambda)| \leqq \| R(f,\lambda) \|_1 \leqq K_\lambda{}^{10} J_f{}'.$$

Since K_λ is uniformly bounded over every compact subset of Λ^*, the same is true of the sequence $F_n(\lambda)$. As $F_n(\lambda) \to F(\lambda)$ for every $\lambda \in \Lambda^*$, it therefore follows that F is analytic in Λ^*.

LEMMA 30. *Let f be a bounded function with compact support on G and $\psi(a,\lambda)$ the function defined by* (10.3). *Then the function*

$$H(\lambda) = \int_G f(a)\psi(a,\lambda)\,da \tag{10.6}$$

is analytic in Λ^*.

Proof. Recall that if $\lambda = (m_1, m_2, \cdots, m_n; s_1, s_2, \cdots, s_n)$ then

$$\lambda(c) = \prod_{j=1}^{n} \left(\frac{c_j}{|c_j|} \right)^{m_j} |c_j|^{s_j}.$$

Furthermore

$$H(\lambda) = \sum_p \int_G \lambda(p^{-1}cp) \frac{f(a)}{D(a)}\,da$$

and $\dfrac{f(a)}{D(a)}$ is integrable and has compact support. The analyticity of H, i.e., the existence of the complex derivatives $\dfrac{\partial H}{\partial s_1}, \cdots, \dfrac{\partial H}{\partial s_{n-1}}$, follows by straightforward differentiation under the integral sign, these operations being justified by the absolute convergence of the integrals in question.

Proof of Theorem 5. If λ is a unitary character, then by its definition $a \to R(a,\lambda)$ is unitarily equivalent to the corresponding representation $a \to T(a,\lambda)$ of the principal series. Thus if f is the convolution of two bounded functions with compact support on G then

$$\operatorname{tr} R(f,\lambda) = \operatorname{tr} T(f,\lambda), \quad \lambda \in \Lambda.$$

On the other hand, Gelfand and Neumark have shown that

$$\operatorname{tr} T(f,\lambda) = \int_G f(a)\psi(a,\lambda)\,da = H(\lambda).$$

But if $F(\lambda) = \operatorname{tr} R(f, \lambda)$ then F is analytic in Λ^*, by Lemma 29 while H is analytic in Λ^*, by Lemma 30. Since $F(\lambda) = H(\lambda)$ for $\lambda \in \Lambda$, i. e., for unitary characters, it follows from Lemma 25 that $F(\lambda) = H(\lambda)$ for all λ in Λ^*. This finishes the proof of Theorem 5.

Proof of Theorem 6. Suppose $R(a, \lambda_1) = AR(a, \lambda_2)A^{-1}$ where A is a bounded operator with a bounded inverse. Then if

$$R(f, \lambda) = \int_G f(a) R(a, \lambda)\, da, \quad \lambda \in \Lambda^*$$

it follows that, $R(f, \lambda_1) = AR(f, \lambda_2)A^{-1}$. Now let f be the convolution of two bounded functions with compact support. Then $R(f, \lambda_1)$ and $R(f, \lambda_2)$ are both of trace class and by a standard property of the trace we see that

$$\operatorname{tr}(R(f, \lambda_1)) = \operatorname{tr}(R(f, \lambda_2)).$$

Thus by Theorem 5

$$\int_G [\psi(a, \lambda_1) - \psi(a, \lambda_2)] f(a)\, da = 0. \tag{10.7}$$

By a simple limiting argument (10.7) also holds whenever f is bounded and has bounded support. Hence $\psi(a, \lambda_1) = \psi(a, \lambda_2)$ a. e.. From this, (10.3) and the continuity of λ_1 and λ_2 we conclude that

$$\sum_p (p\lambda_1)(c) = \sum_p (p\lambda_2)(c)$$

for all diagonal matrices c in G. But since distinct characters are linearly independent, it follows that $\lambda_1 = q\lambda_2$ for some $q \in S$.

Now suppose $a \to T(a)$ is a unitary representation of G and that $T(a) = AR(a, \lambda)A^{-1}$. Then since $T^*(a) = T^{-1}(a) = T(a^{-1})$, we see that

$$A^{*-1}R(a, \lambda)^* A^* = AR(a^{-1}, \lambda)A^{-1}$$

or in other words, that

$$R(a, \lambda)^* A^* A = A^* A R(a^{-1}, \lambda).$$

But when $a \in G_0$, $R(a, \lambda)$ is unitary and irreducible. This implies $A^*A = cI$, where $c > 0$. After proper normalization we may therefore assume A is a unitary operator. Hence $a \to R(a, \lambda)$ is a unitary representation. It follows from Theorem 4 that $R(a, \lambda) = R(a, \lambda')$ where λ' is the contragredient of λ. Thus by the first statement of the present theorem, $\lambda' = q\lambda$ for some q in S.

BRANDEIS UNIVERSITY, AND
THE UNIVERSITY OF CHICAGO.

REFERENCES.

[1] S. Bochner, *Harmonic Analysis and the Theory of Probability*, University of California Press, 1955.

[2] Chevalley, *Theory of Lie Groups* I, Princeton University Press, 1946.

[3] I. M. Gelfand and M. A. Neumark, *Unitäre Darstellungen der Klassischen Gruppen*, Berlin Akademie-Verlag, 1957 (Mathematische Monographien, Band 6).

[4] R. Godement, "Mémoire sur la Théorie des Caractères dans les Groupes Localement Compacts Unimodulaires," *Journal de Mathematiques pures et appliquées*, vol. 30 (1951), pp. 1-110.

[5] ———, "A Theory of Spherical Functions," I, *Transactions of the American Mathematical Society*, vol. 73 (1952), pp. 496-556.

[6] Harish-Chandra, "Representations of Semi-simple Lie Groups, III," *Transactions of the American Mathematical Society*, vol. 76 (1954), pp. 234-253.

[7] E. Hille, *Functional analysis and semi-groups*, American Mathematical Society Colloquium Publications, Vol. 31, 1948.

[8] R. A. Kunze and E. M. Stein, "Uniformly Bounded Representations and Harmonic Analysis of the 2 × 2 Real Unimodular Group," *American Journal of Mathematics*, vol. 82, no. 1 (1960), pp. 1-62.

[9] L. H. Loomis, *An Introduction to Abstract Harmonic Analysis*, D. Van Nostrand Co., Inc., New York, 1953.

[10] E. C. Titchmarsh, *The theory of functions*, second edition, Oxford University Press, 1939.

R. H. Bing has posed the question: if a point-like decomposition of E_3 yields a 3-manifold, must it be E_3? Another question would be: if Y is a 3-manifold and f maps E_3 onto Y such that point inverses are point-like, then must Y be E_3? If a set is point-like, it is cellular (see [2]) and by the continuity of Cech homology, must have the homology of a cell, i. e., must be acyclic. Thus by Corollary 2, these two questions are the same. At any rate, the question is partially answered here. The author thanks R. McMillan for his assistance.

THEOREM 2. *Suppose that Y is a contractible 3-manifold with a locally-finite triangulation and that any finite subcomplex of Y can be semilinearly embedded in E_3. Suppose f maps E_3 onto Y with each $f^{-1}(p)$ a compact absolute retract (i. e. contractible and locally contractible). Then Y is homeomorphic to E_3.*

Proof. If Y is the monotonic union of closed 3-cells, each containing the previous in its interior, then Y is homeomorphic to E_3. Thus it will suffice to show that for each compact subset N of Y, $\exists$ a 3-cell containing N.

Suppose $N \subset Y$ is compact. By Theorem 1, $f^{-1}(N)$ is compact. Let M be the saturation of a closed 3-cell containing $f^{-1}(N)$. Let 0 be the unbounded complementary domain of M and note that $\pi_2(0) \neq 0$. Since f is compact, Smale's theorem (see [5]) applies and $\pi_2(f(0)) \neq 0$. Now by the sphere theorem ([4] and [7]), there exists a polyhedral 2-sphere S in $f(0)$ which cannot be shrunk to a point in $f(0)$. It plus its bounded complementary domain $I(S)$ can be embedded in E_3 by hypothesis, and by Alexander's theorem, S must bound a 3-cell; thus $S \cup I(S)$ is a 3-cell. Since S can be shrunk in $S \cup I(S)$, $I(S) \cap f(M) \neq \phi$, and since M is connected, $f(M) \subset I(S)$ and therefore $N \subset I(S)$. Q. E. D.

The Poincaré conjecture is equivalent to the following: if Y is a contractible 3-manifold, then each compact subset of Y can be embedded in E_3. This is contained implicitly in [3]. R. McMillan and J. Kister have constructed a contractible 3-manifold such that each compact subset can be embedded in E_3, but the manifold itself cannot be (yet unpublished).

INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[1] E. G. Begle, "The Vietoris mapping theorem for bicompact spaces," *Annals of Mathematics*, vol. 41 (1950), pp. 534-543.

[2] M. Brown, "A proof of the generalized Schoenflies theorem," *Bulletin of the American Mathematical Society*, vol. 66, no. 2 (March, 1960), pp. 74-76.

[3] D. R. McMillan, "Cartesian products of contractible open manifolds," *Bulletin of the American Mathematical Society*, Sept., 1961.

[4] C. D. Papakyriakopoulos, "On Dehn's lemma and the asphericity of knots," *Annals of Mathematics*, vol. 66, no. 1, July, 1957.

[5] Stephen Smale, "A Vietoris mapping theorem for homotopy," *Proceedings of the American Mathematical Society*, vol. 8 (1957), pp. 604-610.

[6] L. Vietoris, "Über den höheren zusammenhang kompakter räume," *Mathematische Annalen*, vol. 97 (1927), pp. 454-472.

[7] J. H. C. Whitehead, "On 2-spheres in 3-manifolds," *Bulletin of the American Mathematical Society*, vol. 64 (1958), pp. 161-166.

[8] G. T. Whyburn, "Compactness of certain mappings," *American Journal of Mathematics*, vol. 81, no. 2 (1959), pp. 306-314.

[9] ———, "Analytic Topology," *American Mathematical Society Colloquium Publication*, vol. 27, 1942.

INDEX

PAGE

AUSLANDER, LOUIS. Bieberbach's theorem on space groups and discrete uniform subgroups of Lie groups, II, ... 276

BISHOP, ERRETT. Mappings of partially analytic spaces, ... 209

BISHOP, ERRETT. Some global problems in the theory of functions of several complex variables, ... 479

BISHOP, ERRETT. Partially analytic spaces, ... 669

BLATTNER, ROBERT J. On induced representations, ... 79

BLATTNER, ROBERT J. On induced representations II: infinitesimal induction, ... 499

BOTT, RAOUL and HANS SAMELSON. Correction to "Applications of the theory of Morse to symmetric spaces," 207

BRUHAT, FRANÇOIS. Sur les répresentations des groupes classiques $\mathfrak{p}$-adiques I, ... 321

BRUHAT, FRANÇOIS. Sur les répresentations des groupes classiques $\mathfrak{p}$-adiques II, ... 343

COHEN, ECKFORD. Arithmetical notes, V. A divisibility property of the divisor function, ... 693

COHN, HARVEY. Calculation of class numbers by decomposition into three integral squares in the fields of $2^{\frac{1}{2}}$ and $3^{\frac{1}{2}}$, . . . 33

CONNELL, E. H. Images of E_n under acyclic maps, ... 787

EDWARDS, C. H., JR. Polyhedra in S^n whose complements have uniformly Abelian local fundamental groups, ... 557

FALB, PETER. See Oscar Zariski and Peter Falb, page 542.

FURSTENBERG, H. Strict ergodicity and transformation of the torus, 573

GORDON, BASIL. A combinatorial generalization of the Rogers-Ramanujan identities, ... 393

GORENSTEIN, DANIEL and I. N. HERSTEIN. Finite groups admitting a fixed-point-free automorphism of order 4, ... 71

HAEFLIGER, ANDRÉ. Points multiples d'une application et produit cyclique reduit, ... 57

HARTMAN, PHILIP. On differential equations and the function $J_\mu^2+Y_\mu^2$, 154

HERSTEIN, I. N. See Daniel Gorenstein and I. N. Herstein, page 71.

HERTZIG, DAVID. The structure of Frobenius algebraic groups, . . 421

PAGE

Hochschild, G. and G. D. Mostow. On the algebra of representative functions of an analytic group, ... 111

Iseki, Shô. Partitions in certain arithmetic progressions, . . 243

Klingenberg, Wilhelm. Lineare gruppen über lokalen ringen, . 137

Klingenberg, Wilhelm. Orthogonale gruppen über lokalen ringen, 281

Kunze, R. A. and E. M. Stein. Uniformly bounded representations, II, 723

Lewis, D. C. Autosynartetic solutions of differential equations, . 1

Mattuck, Arthur. Symmetric products and Jacobians, ... 189

Mostow, G. D. See G. Hochschild and G. D. Mostow, page 111.

Mumford, David. Pathologies of modular algebraic surfaces, . . 339

Murre, J. P. On Chow varieties of maximal, total, regular families of positive divisors, ... 99

Narasimhan, M. S. and S. Ramanan. Existence of universal connections, ... 563

Palais, Richard S. and Thomas E. Stewart. The cohomology of differentiable transformation groups, ... 623

Ramanan, S. See M. S. Narasimhan and S. Ramanan, page 563.

Ratliff, Louis J., Jr. Affine rings over rank two regular local rings, 709

Ree, Rimhak. A family of simple groups associated with the simple Lie-algebra of type (F_4), ... 401

Ree, Rimhak. A family of simple groups associated with the simple Lie algebra of type (G_2), ... 432

Ringrose, J. R. Algebraic isomorphisms between ordered bases, . 463

Saito, Masahiko. Sous-groupes discrets des groupes resolubles, . 369

Samelson, Hans. See Raoul Bott and Hans Samelson, page 207.

Seeley, R. T. Regularization of singular integral operators on compact manifolds, ... 265

Seeley, R. T. On boundary value problems for Laplace's equation, 698

Shapiro, H. S. and A. L. Shields. On some interpolation problems for analytic functions, ... 513

Shields, A. L. See H. S. Shapiro and A. L. Shields, page 513.

Stein, E. M. See R. A. Kunze and E. M. Stein, page 723.

Stewart, Thomas E. See Richard S. Palais and Thomas E. Stewart, page 623.

PAGE

TREVES, FRANÇOIS. An invariant criterion of hypoellipticity, . . 645

TULLY, E. J., JR. Representation of a semigroup by transformations acting transitively on a set, ... 533

WHITE, A. J. On the summability, by spherical Riesz means, of derived multiple Fourier series, ... 602

ZARISKI, OSCAR and PETER FALB. On differentials in function fields, 542